State of Maine
Information Technology
Security Policy

Version 1.2

Office of
The Chief Information Officer

January 6, 2009

Table of Contents

1. Common Policy Elements

1.1 Introduction and Scope

State information is a valuable asset that must be protected from unauthorized disclosure, modification, use, or destruction. Prudent steps must be taken to ensure that its integrity, confidentiality, and availability are not compromised.

This document provides a uniform set of information technology security policies, standards and general guidelines for every State Department, Agency, Board, Bureau, Commission, and Authority which are required to comply with Maine Revised Statute Annotated (MSRA) Title 5, Chapter 163 §§ 1971-2011. All Maine State Government entities, unless specifically exempted, are required to abide by the policies hereby established. All users (employees, contractors, vendors, and other parties) are expected to understand and abide by them.

In addition to defining roles and responsibilities, information security policies raise awareness of users to the potential risks associated with information technology. Employee awareness through dissemination of the policies helps minimize the cost of security incidents, accelerate the development of new application systems, and assure the consistent implementation of controls for information systems throughout the organization.

The State of Maine enterprise information technology security policies are based upon the ISO 17799 standard framework and include explanatory guidelines for clarification. The policies are designed to comply with applicable laws and regulations, however, if there is a conflict, applicable laws and regulations will take precedence. The policy statements should be considered minimum requirements for providing a secure environment for developing, implementing, and supporting information technology and systems. Associated enterprise standards coinciding with certain policies must be adhered to by Agencies unless specifically granted an exception. Agencies must develop detailed policies and procedures to handle Agency-specific cases.

1.2 Authority

The Maine Chief Information Officer was created by an act of the Legislature to *"...Set policies and standards for the implementation and use of information and telecommunications technologies, including privacy and security standards..."* and to *"provide central leadership and vision in the use of information and telecommunications technology on a statewide basis."* (MRSA, Title 5, Chapter 163, § 1973). All Information Technology policies and standards are subject to approval by the CIO. These enterprise technology security policies and standards are established under such authority to assist State Agencies to more effectively manage the State of Maine information technology resources and systems managed by them.

1.3 Enforcement

Individual State Agencies will be responsible for complying with these security policies and standards. These policies and standards will guide periodic security reviews, as well as audits.

In addition, the Chief Information Officer, in conjunction with the Bureau of Purchases, will review applicable equipment and service purchases to ensure that vendors and contractors are aware of the security policies and standards and have agreed to comply with them. Violators of these policies may be subject to employee disciplinary procedures. Agencies may impose additional sanctions upon their employees for violations of these policies and standards.

1.4 Exceptions

Exceptions to these policies must be approved by the Enterprise Information Security Director (EISD). In each case, the Agency or vendor must request the exception, in writing, and include such items as the need for the exception, the scope and extent of the exception, the safeguards to be implemented to mitigate risks, specific timeframe for the exception, organization requesting the exception, and the approval from the Agency head requesting the exception. Denials of requests for exceptions may be appealed to the CIO.

The policies described in this manual are applicable to all information technology systems. Generally, internal test and experimental systems not connected to a production network do not require the same level of security. Applications development systems may also be exempt, provided they are on a physically separate, non-production network. If these development or test systems are on the same network as production systems, however, they must follow the same security policies as production systems.

1.5 Version History

As policies are revised or updated, a version history summarizing the changes shall be listed as the last section of the policy document. The Version History section shall also list revisions or updates to enterprise security standards. The Version History section will be similar to the example shown below:

> **VERSION HISTORY**
> **Original Policy** established June 4, 2002
> **Revised** December 19, 2002.**1.6 Related Documents**

Appendix A contains a listing of documents related to the State of Maine enterprise information technology security policies. This list should not be considered all inclusive. The enterprise information technology security policies and appropriate related documents must be considered collectively toward establishment of an effective IT Security Program.

2. Terms and Definitions

This section includes some of the important terms referenced in the various enterprise information security policies. Additional terms may be defined within each individual policy.

Term	Definition

Term	Definition
Access Control List (ACL)	A table that tells a system what access rights are granted based on a specific identification parameter such as user-id, network segment, or host name.
Agency, Agencies or the State of Maine	Every State Department, Agency, Board, Bureau, Commission, and Authority which are required to comply with Me. Rev. Stat Ann. Title 5, Chapter 163.
Automated Terminal Identification (ATI)	Any method of identifying a specific device used for allowing user access to a secured information system. ATI is separated from user identification so that an extra layer of security may be provided when deemed necessary.
Biometrics	Refers to the use of electro-mechanical devices that measure some physical, electrical or audio characteristic of an individual and make use of that specific measurement to verify identity.
Change Management	A business process that ensures that no changes occur on a computing resource without having gone through a methodology to ensure that change will perform as expected, with no unexpected repercussions.
Criminal Justice Information Systems (CJIS)	Manages a series of computerized information systems that index criminal justice information concerning crimes and criminals of State and national interest.
Digital Certificate	A file of encrypted data that has been issued to an individual user and verifies that the user is who they claim to be. The user engages the digital certificate by means of a password and can be used to 'sign' communications that verify the identity of the user to others.
Health Insurance Portability and Accountability Act of 1996 (HIPAA)	This act mandated regulations that govern privacy, security, and electronic transactions standards for health care information.
Information Processing Facilities or Information Processing and Communication Facilities	A facility that contains a data center, network operations center, or other similar information system command or monitoring center with computer systems that store production information or house network services or user workstations.

Term	Definition
Information Security	Preservation of *confidentiality, integrity, and availability* of information. *Confidentiality* - Ensuring that information is accessible only to authorized users *Integrity* - Safeguarding the accuracy and completeness of information and processing methods *Availability* - Ensuring that authorized users have access to information and associated assets when required
Information Security Incident or Breach	An event that results in unauthorized access, loss, disclosure, modification or destruction of information resources whether accidental or deliberate.
Information System	The network or combinations of all computing equipment, telecommunication or other communication or information processing devices and channels used within an organization.
Open Source Software	Software that is written by authors who submit it for use by the general public without requiring payment for the software. Typically available as downloadable code from the Internet as unsupported code.
Private Key	A small, encrypted file that is used to identify a user by means of a pass phrase or password. The successful use of the password or phrase will then allow the decrypting of information generated from the matching public key. The private key is also used to create a digital signature that can be decrypted by anyone with the corresponding public key to confirm that the key owner "signed" the document.
Public Key	A small, encrypted file that contains information about a specific user. The public key is supplied by the owner to anyone wishing to encrypt a document or message so that only the public key owner can decrypt it using their private key. For digital signatures, the public key is used to confirm that the message was signed electronically by the owner using their private key.

Term	Definition
Risk Assessment	Assessment of threats to, impacts on, and vulnerabilities of information and information processing facilities.
Risk Management	Process of identifying, controlling, and minimizing or eliminating security risks that may affect information systems
SLA- Service Level Agreement	A detailed subsection of a contract that specifies expected services, procedures and responses
Smart Card	A physical card that contains some electrically responsive capability that indicates its unique identity. Combined with a User ID and password, a Smart Card helps verify a given user.
Teleworking/Telecommuting	The practice of working from a site that is remote from the user's normal base office but still within a more controlled environment than a typical remote dial-in or internet connection. Teleworking allows staff to work from a fixed location that is remote from the organization's base operation.
Token	A device that operates much like a smart card but is in a physical shape that makes its use easier to manage. A special ring worn on the hand is one form of a token.
Trojan Horse	Software that is written to allow access to a computer via some method not intended by the owner of the system. Typically embedded in some other form of software Trojan code attempts to camouflage its presence to avoid detection. Trojan code operates by either announcing itself to the writer of the code when installed or by responding to a special form of prompting. The intent of the code is to allow access to a computer without the knowledge of the computer owner.
Trust Model	A trust model is the system of hardware, software and procedures by which any organization may establish how information is authenticated, verified or secured from disclosure.
Users	Employees, contractors, vendors, or any other parties who are granted access to a State of Maine production system or application

3. Security Policies

3.1 Information Technology Security Policies

3.1.1 Information Technology Security Policies Document

INFORMATION TECHNOLOGY SECURITY POLICIES DOCUMENT	
POLICY NUMBER: **3.1.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

> ➢ To broadly define information technology security.
> ➢ To demonstrate the State's commitment to best practices for ensuring security of information technology, data, and information systems.

SCOPE

All users are expected to understand and abide by established enterprise information technology security policies.

POLICY

> *State information is a valuable asset and must be protected from unauthorized disclosure, modification, or destruction. Prudent information security policies, standards, and practices must be implemented to ensure that the integrity, confidentiality, and availability of State information are not compromised.*

STANDARDS

Standards are specific directives, specifications, or procedures that must be followed in order to ensure a consistent implementation of information technology security practices.

GUIDELINES

Guidelines are intended to aid users in understanding and applying the policies. Guidelines set forth best practices or recommended courses of actions. Guidelines will be incorporated into Agency policies and standards to the fullest extent possible.

Policies:
> ➢ Identify general areas of risk.
> ➢ State generally how to address the risk.
> ➢ Provide a basis for verifying compliance through audits.
> ➢ Be realistic and enforceable.
> ➢ Be concise and easy to understand.
> ➢ Balance protection with productivity.

Standards:
- ➢ Set forth minimum requirements designed to address certain risks.
- ➢ Set forth specific requirements that ensure compliance with policies.
- ➢ Provide a basis for verifying compliance through audits.
- ➢ Be realistic and enforceable.
- ➢ Be easy to understand.
- ➢ Balance protection with productivity.

Guidelines:
- ➢ Identify best practices to facilitate compliance.
- ➢ Provide additional background or other relevant information.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Sections 1.2 and 1.3)

TERMS AND DEFINITIONS (see Section 2)

3.1.2   Review and Evaluating

REVIEW AND EVALUATING	
POLICY NUMBER: **3.1.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To identify the owner of State of Maine enterprise information technology security policies and describe the process for reviewing and maintaining them.

SCOPE

All enterprise security policies established by the Chief Information Officer.

POLICY

The Enterprise Information Security Director (EISD) shall be responsible for the policies defined in this document. The EISD, in conjunction with Chief Technology Officer (CTO) and Chief Information Officer (CIO), will periodically review their effectiveness and propose updates, as necessary.

GUIDELINES

Agencies must report operational information security incidents to the Enterprise Information Security Director within the Office of Information Technology. The Chief Information Officer will periodically review these operational incidents to assess the effectiveness of policies and standards and identify possible new vulnerabilities.

The effectiveness of the policies defined in this document must consider the following:
- ➢ The nature, number, and impact of recorded security incidents.

➢ The cost and impact of controls on business efficiency, including third-party vendor compliance.
➢ The effects of changes to organizations or information technology.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

4. Organizational Security

4.1 Information Security Infrastructure

4.1.1   Information Security Infrastructure

INFORMATION SECURITY INFRASTRUCTURE	
POLICY NUMBER: **4.1.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance in establishing the basic elements of information technology security infrastructure. Security infrastructure is the complete set of information security-related systems, procedures, policies and physical implementations of information technology security administration within each Agency.

SCOPE

All Agencies of the State Government of Maine.

POLICY

Agencies that create, use or maintain information systems for the State of Maine shall create and maintain an information security infrastructure that ensures the confidentiality, availability, and integrity of the State's information assets.

STANDARDS

Agencies must meet the following standards:
➢ Appoint or designate, in writing to theEnterprise Information Security Director (EISD), an Information Technology Security Officer to administer an information technology security program to ensure the confidentiality, integrity and availability of State information technology assets.
➢ Implement and maintain a minimum program based upon the State of Maine Enterprise Information Technology Security Policy and the ISO 17799.
➢ Implement additional policies and procedures as necessary to meet security requirements imposed on such Agency by Federal or other State security requirements.
➢ The Agency Information Technology Security Officer shall be responsible for ensuring

their Agency's implementation of Enterprise Security Policies and Standards as adopted by the CIO.
- ➢ Each Agency Information Technology Security Officer shall serve as the primary Agency point of contact to the Enterprise Information Security Director for all Information Technology Security matters.

GUIDELINES

General

The Agency Information Technology Security Officer will be the focal point for all IT security related matters.

Information Security Management

As required by this policy, an Agency Information Technology Security Officer must be designated. Depending on the organization's size and complexity, this role may require a significant amount of effort. The Information Technology Security Officer must oversee all information technology security-related events and information.

The Agency Information Technology Security Officer should report to the Commissioner, Agency Head, or other similar executive-level business manager.

The business management of an organization ultimately benefits or suffers from information technology security issues. Therefore, clear lines of responsibility and organizational roles must be defined to properly administer the functions of information security. In establishing these functions, the following issues shall be addressed:
- ➢ Formulation, review and approval of Agency information technology security procedures.
- ➢ Maintenance of threat assessments for internal information.
- ➢ Oversight of investigations into computer security-related incidents.
- ➢ Development and testing of Business Continuity and Disaster Recovery planning.
- ➢ Oversight of business issues regarding information technology security initiatives.

Information Security Coordination

In large organizations, it may be necessary for multiple subgroups to maintain their own information technology security functions. In this case, the coordination of these groups is essential for overall information technology security. Policies and procedures for the entire organization will:
- ➢ Define the roles and responsibilities of the various groups.
- ➢ Establish methodologies, procedures, processes, risk assessment and information classification guidelines.
- ➢ Provide information technology security user education.
- ➢ Provide security-related technical architecture to planning and development groups.
- ➢ Designate security incident investigation responsibility.

> ➢ Provide identification of an architectural interface to the business management groups.

Allocation of Information Technology Security Responsibilities

Clear assignment of responsibilities for various security related issues is critical to the success of information technology security. Delegating responsibility for security throughout the organization is a good method of ensuring a cohesive approach to policy management. For each area of security responsibility the following issues should be addressed:

> ➢ For any individual information technology system, the security processes for the assets and access should be clearly established in a documented form.
> ➢ The responsibility, or owner, of each asset and the security process for gaining access to the asset should be clearly defined.
> ➢ Authorization levels for access to assets should be clearly defined.

Authorization for Information Processing Facilities

The management of an organization bears the responsibility for approval of new information processing facilities. These facilities may be defined as a complete data center or a single laptop. The approval process should involve information technology security organization. Regardless of the computing resource's size or complexity, compliance of the security environment with existing security policy should be evaluated. When approving new information processing facilities, the following issues (at a minimum) should be addressed:

> ➢ Assessment of the ability of the new processing facilities to conform to existing security policy, including any additional State and Federal requirements.
> ➢ Evaluation of hardware and software compatibility of the new facilities with existing facilities.
> ➢ Evaluation of the need for additional security measures and the impact of personal computing systems.
> ➢ Assessment of Business Continuity and Disaster Recovery planning by the Office of Information Technology where a new data center is proposed.

Third Party Assessment

The use of information security specialists to guide and oversee the information security infrastructure is important to maintain awareness of new security-related threats and other issues. Where in-house expertise is not available, external resources such as the Office of Information Technology Security Office or private-sector resources may add value. In cases of security-related investigations, such external resources may be required.

Cooperation Between Organizations

The information technology security administration should maintain contact lists of both internal and external organizations and service vendors. These lists should be organized to quickly facilitate security-related events and investigations. They should detail the management staff authorized to make decisions regarding security-related events.

Membership in security-related organizations may provide valuable insight into the ongoing practices of security administration. However, the release of State security events and issues must be approved by business management and information technology security administration.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

4.2 Security of Third Party Access

4.2.1 Identification of Risks From Third Party Access

IDENTIFICATION OF RISKS FROM THIRD PARTY ACCESS	
POLICY NUMBER: **4.2.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance for allowing third party access to State of Maine computing resources. This policy addresses the issues surrounding the level of security risks taken as a result of third party access.

SCOPE

Any State of Maine organization that allows a third party access of any type into State of Maine information technology resources.

POLICY

Risk identification and assessment must be done and documented prior to establishing third party access to State of Maine information technology systems and must be in accordance with the policies set forth in Section 9. Access Control.

GUIDELINES

Third party access into State computing resources may come in many different ways. For each of the various ways there are differing risks to be examined and dealt with. The most significant type of access will be a network-to-network connection that allows multiple users or systems from the third party to interact with State resources. Simpler methods of network access include connection of devices such as laptops. Managing the risk involved in these situations is something that must be done prior to making the connections available.

The third party should be provided with a copy of the information technology security policy and be required to comply. Alternatively, a contracted information technology security contractor may be used to examine the third party systems and provide a determination that they present no additional risk to State of Maine resources.

Type of Access

The types of access that third parties may have into State resources fall into two primary categories. The first category is that of Physical access. In many cases, this will take the form of a contractor working on State premises to serve some particular need. The work the contractor is doing may not be related to computing resources, but, if State computing resources are physically co-located then some risk exists. In many cases the contractor will be working directly on the computing systems themselves and will have been granted some sort of user account. When contractors have user accounts on State systems they must meet and follow the same standards as regular State employees.

Network connection ports should be monitored for unknown devices and un-authorized connections. Detailed map of physical and logical network connections should be available to the information technology security administration.

When contract personnel are working in a State environment without being directly supervised, then State employees must be vigilant about logging off sessions, logging out or securing PC access, and keeping paper information properly discreet.

The second category is that of Logical access. It involves the contractor coming into State resources via some external capability. This may be a remote dial-in, a connection through a firewall, or even a login through a direct network connection. While logical access presents a very cost effective way of using third party resources, it presents a significant risk in that it is more difficult to monitor the actions of the third party. Very tight controls must be required on user accounts using remote logical access. Where the third party access will involve a network-to-network connection, the Agency must coordinate with OIT to ensure the use of control and filter mechanisms (such as a firewall). When contractors have user accounts on State systems they must meet and follow the same standards as regular State employees.

Reasons for Access

The reasons for granting access to third parties are typically driven by a business need. This includes use of services provided by third parties to develop software or maintain systems. The management of the associated risks is the responsibility of the State Agency that is sponsoring the third party access. When the use of third party access is deemed necessary, the account management for this access must be scrutinized. Where the operating system is capable of tightly controlling user access, a complete user profile should be constructed that addresses the following minimum criteria:
  ➢ Time of day access.
  ➢ Day of week access.
  ➢ Physical location access.
  ➢ Networked location access.
  ➢ Direct dial in access.
  ➢ User directory permissions.
  ➢ User application access.

A complete record of access granted and its usage should be documented. This is required when the third party access will include access to State information that is considered highly sensitive. Extra safeguards and account considerations should be used to manage risk of this type.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

4.2.2   Security Requirements in Third Party Contracts

SECURITY REQUIREMENTS IN THIRD PARTY CONTRACTS	
POLICY NUMBER: **4.2.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance on the information technology security issues that should be considered when using third party resources to accomplish State business. No third party access to State resources should take place without first having entered into a binding contract that clearly delineates the security responsibilities of the third party.

SCOPE

Any situation in which an Agency of the State of Maine uses resources from third parties to access and perform work with State computing resources.

POLICY

> *Any contract with a third party entity that involves access to State of Maine information resources will delineate State information security issues relevant to that business access and require the third party to adhere to enterprise information security policies and standards.*

GUIDELINES

When writing contracts with third parties to provide any type of services that involve accessing State of Maine computing resources, the Agency involved bears the burden of ensuring that all relevant information security issues have been addressed. Using the State of Maine Enterprise Information Technology Security Policy as a reference is recommended. Provisions in the contract requiring the third party to demonstrate their ability to meet the requirements of the State information security policy will provide a basis of trust for further technical interaction.

Onsite Contract Resources

When a third party service provider will be placing contract resources on State premises, security issues may occur related to the actions of the contracted personnel. The contract should reflect the acceptance by the third party of responsibility for the actions of its members. The contract should also reflect that the burden is on the contracting organization to provide due diligence in

determining the skills and character background of the onsite personnel.

Logically Connected Contract Resources

When a service provider will be using a logical connection to State resources, the contract must outline the responsibilities of the third party users and the security integrity of any connected networks, systems or logons. The third party provider must be able to demonstrate ability to meet or exceed normal State information technology security policies and guidelines.

Specific Contract Issues to be Addressed

Third party contracts should contain sections that address the following issues:
  - State of Maine Information Technology Security Policy.
  - Asset protection.
    - Protection procedures for both hardware and software assets.
    - Procedures for determining any compromise of assets.
    - Verifiable procedures for the destruction and/or return of State information assets at the end of the provided service.
    - Systems integrity and availability.
    - Specific restrictions on copying or disclosing State information.
  - A detailed description of each service to be offered.
  - Service level criteria for acceptable and non-acceptable performance.
  - Detailed provisions for transfer of staff as required.
  - Liabilities for both the service provider and the State.
  - Specific provisions as to delegate responsibilities in legal issues involving other organizations and provisions of law.
  - Provisions for distribution of intellectual property rights and collaborative work
  - Detailed access control agreements, to include:
    - Provisions for granting access and the management of unique user and system identifiers.
    - A process for granting authorized user access.
    - Methodology for managing authorized user lists and access rights across systems
  - Performance criteria with monitors and verifiable definitions.
  - Privilege management of user access, monitoring user activity, and the State's right to refuse access.
  - The rights to monitor contractual compliance and the right to use third parties to establish contractual compliance.
  - A process for escalating service issues, problem resolution and contingency plans.
  - Detailed descriptions of responsibilities regarding hardware and software installation and maintenance.
  - A clearly defined reporting structure and specific reporting formats and expected content.
  - A detailed plan for change management procedures.
  - Detailed descriptions of physical protection methods and procedures for verifying compliance.
  - A detailed plan describing the educational process for users and administrators in methods, procedures and security.

- ➢ Systems plan for control of malicious software.
- ➢ A procedure for reporting and investigating security related issues and escalation procedures.
- ➢ Responsibilities of the provider with sub-contractors.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

REFERENCES:
1. Rider B54 EO-IT (Item 39 – State IT Policies) **-**
   http://www.maine.gov/purchases/forms/BP54 EO-IT.doc
2. Deployment Certification Policy for Major Application Projects (payment holdbacks to be included in contracts dependant on certification of application) - http://www.maine.gov/oit/oitpolicies/DeployCertPolicy.htm

4.3 Outsourcing

4.3.1   Security Requirements in Outsourcing Contracts

SECURITY REQUIREMENTS IN OUTSOURCING CONTRACTS	
POLICY NUMBER: **4.3.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance when using third party service providers to manage and maintain State of Maine information computing resources.

SCOPE

Any circumstance where an Agency of the State of Maine will sign binding contracts with a service provider to outsource specific responsibilities for maintenance of State information resources.

POLICY

Any outsourcing agreement will contain information technology security provisions specifically tailored to the particular outsourcing initiative.

GUIDELINES

The relationship of an outsourced service provider to the State should be based on a very detailed contract that delineates specific responsibilities of the provider and the expectations of the State. These contracts will contain sections that are known as Service Level Agreements (SLA's).

These SLA's must outline the expected services and detailed responses to specific issues.

Information security issues should be included or addressed in the SLA's as an expectation by the State that the provider will meet or exceed all of the policies stated within the State of Maine information security policy. The security provisions of an outsourcing contract should address the entire technical topology of the outsourced environment. When engaged in agreements with outsourcing providers, the use of specific SLA's and security compliance verification should exist with in the contract.

Contract provisions

Specific information technology security provisions of an outsource contract should address the following issues:
  ➢ Verifiable criteria for how the legal requirements are to be met.
  ➢ Plan for educating all contract parties in security related responsibilities and procedures.
  ➢ Verifiable criteria for how State assets are to be maintained and tested.
  ➢ Control procedures for granting authorized and managed access to users.
  ➢ Disaster recovery and business continuity issues.
  ➢ Physical security arrangements for State information assets that exist outside of State premises.
  ➢ Rights of the State to verify contract compliance through the use of audits, tests, and third party examination.
  ➢ The applicable contract terminology addressed in Section 4.2.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

REFERENCES:
  1. Rider B54 EO-IT **-** http://www.maine.gov/purchases/forms/BP54 EO-IT.doc
  2. Remote Hosting Policy http://www.maine.gov/oit/oitpolicies/RemoteHostingPolicy.htm

5. Asset Classification and Control

5.1 Accountability for Assets

5.1.1 Inventory of Assets

INVENTORY OF ASSETS	
POLICY NUMBER: **5.1.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance for accountability regarding physical computing assets of the State of Maine. The asset inventory is defined as the means by which the hardware and software assets are accounted for within the State of Maine.

SCOPE

Hardware computer and communications devices, software packages, and user licenses acquired for use by the State of Maine.

POLICY

All hardware and software operated by agencies of the State of Maine will be documented in compliance with all applicable State or Agency asset management policies and associated statutes.

GUIDELINES

Asset inventory is the method by which the State maintains knowledge of the physical devices and software purchased with public funds. As devices and software become out of date or no longer in use they should be removed from the inventory lists in accordance with State asset management procedures for each State entity.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

5.2   Data Classification

5.2.1   Data Classification Guidelines

DATA CLASSIFICATION GUIDELINES	
POLICY NUMBER: **5.2.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To establish policies for the classification of electronically-stored State of Maine information and data.

SCOPE

All information contained within computing resources operated by Agencies of the State of Maine.

POLICY

Each Agency must adopt and adhere to an information classification system, that includes the extent to which information on State of Maine computer systems should be disclosed to specified users, consistent with applicable State and Federal access, privacy and

confidentiality statutes.

GUIDELINES

Classifications and associated protective controls for information should consider the business needs for sharing or restricting information, and the business impacts associated with such needs, e.g. unauthorized access or damage to the information. In general, the classification given to information is a shorthand way of determining how this information is to be handled and protected. The following general categories of information serve to provide guidance in identifying appropriate users or recipients:
  ➢ Public Information – information accessible under Freedom of Information Law is available to any person, notwithstanding individual status or interest.
  ➢ Restricted Information – information which is not public information, but can be disclosed or used by agency representatives to carry out their duties, as long as there is no legal prohibition to disclosure.
  ➢ Confidential Information – Information which is protected by law. Access to confidential information is prohibited unless permitted by an exception in the law.

Classification of information and outputs from systems handling classified data should consider labeling in terms of its sensitivity and include the following aspects:
  ➢ Information often ceases to be sensitive or critical after a certain period of time, for example, when the information has been made public. Anticipate and allow for the fact that the classification of any given item of information is not necessarily fixed for all time, and may change.
  ➢ Over-classification can lead to an unnecessary additional business expense.
  ➢ Overly complex schemes may become cumbersome and uneconomic to use or prove impractical.
  ➢ Care should be taken in interpreting classification labels on documents from other organizations which may have different definitions for the same or similarly named labels.

The responsibility for defining the classification of an item of information, e.g. for a document, data record, data file or diskette, and for periodically reviewing that classification, should remain with the originator or nominated owner of the information.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

5.2.2   Data Labeling and Handling

DATA LABELING AND HANDLING	
POLICY NUMBER: **5.2.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To address the issue of how electronically-stored data that has been classified should be labeled and handled.

SCOPE

Data that has been classified by any State of Maine Agency.

POLICY

> *Each Agency must adopt and use information labeling and handling procedures in accordance with the information classification scheme adopted by the Agency.*

GUIDELINES

It is important that an appropriate set of procedures are defined for information labeling and handling in accordance with the classification scheme adopted by the organization. These procedures need to cover information assets in physical and electronic formats. For each classification, handling procedures should be defined to cover the following types of information processing activity:

➢ Copying.
➢ Storage.
➢ Transmission by post, fax, and electronic mail.
➢ Transmission by spoken word, using telephone, voicemail, answering machines.
➢ Destruction.

Output from systems containing information that is classified should carry an appropriate classification label (in the output). The labeling should reflect the classification established in 5.2.1. Items for consideration include printed reports, screen displays, recorded media (tapes, disks, CDs, cassettes), electronic messages and file transfers.

Physical labels are generally the most appropriate forms of labeling. However, some information assets, such as documents in electronic form, cannot be physically labeled and electronic means of labeling need to be used.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

6. Personnel Security

6.1 Personnel Security Screenings

6.1.1 Personnel Security Screenings

PERSONNEL SECURITY SCREENINGS	
POLICY NUMBER: **6.1.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To minimize the risks of human errors, fraud, and misuse by addressing information technology security concerns at the recruitment stage of employment for all potential State of Maine employees, and prior to the engagement of contractors.

SCOPE

All Agencies within the State of Maine Government.

POLICY

Agency hiring authorities must conduct personnel screenings of prospective employees and contractors who will be granted access to State of Maine information systems.

GUIDELINES

Job Description and Security Responsibilities

- ➢ Agency hiring authorities will identify the degree of access to state information systems, processes and data in addition to normal roles and responsibilities.
- ➢ Applicable State or Federal regulations or policies, terms of confidentiality, and conditions of employment must be covered along with normal administrative processes during the employment phase of hiring.
- ➢ Disciplinary or criminal procedures will be consistent with existing State administrative regulations, labor union agreements and criminal codes.

Employee/Contractor Screening

Verification checks should be conducted as part of the employment/engagement process for both full- and part-time employees and contractors. Such checks should be repeated periodically in cases of job change, role change, or promotion.

Personnel screening checks must include one or more of the following, depending on the particular job duties, responsibilities, and access privileges of the position:
- ➢ Character references (business and personal, as appropriate).
- ➢ Training background.
- ➢ Academic and professional experience.
- ➢ Identity and background checks.
- ➢ Credit checks, when appropriate.

The sourcing Agency for contractors, consultants, and third-party vendors shall use similar criteria in screening processes, to include:
- ➢ Initial screening.
- ➢ Job-specific screening, if sensitive areas are to be accessed.

➢ Notification of re-screening, as required.

Employee/Contractor Supervision

Managers and supervisors shall evaluate the procedures required for personnel that may be accessing sensitive information. These procedures should be reviewed and updated by senior management or staff, as necessary.

Confidentiality Agreements

Confidentiality and non-disclosure agreements must indicate that certain information is private or secret. Employees who need to access such information should be required to sign these agreements when initially employed. Third-party users who are not already covered by an existing agreement should also sign such agreements prior to being given access to the information.

Confidentiality and non-disclosure agreements should be reviewed regularly, especially when employees leave the organization or when contracts expire.

Terms and Conditions of Employment

Terms and conditions of employment should clearly state the employee's responsibilities for information security. They should include a defined period of time after employment and the actions that will be taken in the event of non-compliance to the agreement.

It may be necessary to specifically include the following items within the offer of employment or contractor agreement:
➢ Employee/Contractor's legal rights and responsibilities regarding copyright laws, data protection legislation.
➢ Data classification and management when working off-site and outside of normal business hours.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

REFERENCES
1. Verification of Eligibility for Employment (Form I-9) - http://www.maine.gov/bhr/rules_policies/policy_manual/5_2.htm

6.2 User Training

6.2.1 Information Security Education and Training

INFORMATION SECURITY EDUCATION AND TRAINING	
POLICY NUMBER: **6.2.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To ensure that users are knowledgeable and aware of security threats, concerns, and the procedures for reporting security incidents.

SCOPE

All agencies, their employees and third parties that access the State of Maine information systems.

POLICY

Information technology security training will be conducted and documented annually for all employees of the Agency. Training will include security awareness, updates to security policies or procedures, and reporting of incidents and vulnerabilities.

GUIDELINES

Access Guidelines

Each organization should create procedures for training all employees and other users on how to access and use its information systems.

All employees should be trained on access controls and legal responsibilities. All employees should be aware and remain vigilant for possible fraudulent activities. Well-defined procedures should be in place in order for employees to report incidents involving their personal accounts or the acts of others.

Software Packages

Training should be conducted on the acceptable use of all software. Policies and procedures are to be developed and delivered in a training arrangement with all employees.

New Systems

Users should be trained on the use of new systems. The level of information security training required for individual system users should be appropriate to their specific duties and be directed to ensure that the confidentiality, integrity, and availability of information is safeguarded.

Technical Staff

While technical staff is entrusted to protect the organization's information, they may also inadvertently (or maliciously) put it at greater risk. Therefore, it is essential that they be trained to a level of competence in information technology security that matches their duties and responsibilities.

Incident Reporting

A process for reporting incidents and concerns should be understood by all employees so they can communicate breaches and all other suspicious activities to the appropriate levels of supervision within the organization.

Information Technology Security Officer

The ultimate responsibility for information technology security within the Agency rests with senior executive management. The Information Technology Security Officer within the Agency will assist with the oversight of the information security administration. This resource has responsibility with safeguarding all Agency information, measuring effectiveness, providing countermeasures, and development of training and awareness programs.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

6.3 Responding to Security Incidents

6.3.1 Reporting Security Incidents

REPORTING SECURITY INCIDENTS	
POLICY NUMBER: **6.3.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To ensure that all State of Maine Agencies have a defined process for their employees to report security incidents so that they can be dealt with quickly to minimize risk to the Agency and the State of Maine.

SCOPE

All State of Maine employees, agencies or third parties that maintain communications systems, computing platforms or hosted applications that contain State of Maine information.

POLICY

Each Agency shall implement a security incident reporting process and train its employees on how to use the process.

GUIDELINES

Development of a Procedure

Each Agency should formally assign responsibility for information technology security to a specific administrator. The responsibility of this role is to oversee all aspects of information security, including all processes, procedures, and methodologies used to monitor and execute information technology security programs. The administrator assigned responsibility for information security should document an incident reporting and handling process to include:

➢ A process for all users to communicate breeches of security and other incidents.
- o The method may require some level of confidentiality and protection for the user initiating the report.
- o All users must be aware of the process.
- o A method of logging and tracking needs to be addressed for the specific incidents.
- o Users should be provided a receipt or some type of acknowledgement that their request has been received as well as updates during the investigative stages.

➢ Documented escalation procedures to inform the appropriate personnel quickly. This should include all responsible parties, system administrators, and management. These escalation procedures should include multiple escalation points depending on the severity of the incident so that evidence can be collected and the damage or restoration can be completed in a timely manner.

➢ A close-out and feedback process to communicate back to the appropriate user when the incident is resolved.

➢ A report process to report incident types, severity levels, access details, and involvement. This should be reported to management and security personnel regularly so that this information can be shared across organizations and used to further enhance training and development processes.

➢ A process for awareness training to educate users of historical incidents to eliminate future incidents from occurring.

Reporting Guidelines

A procedure should be developed for reporting security incidents to outside organizations such as regulatory bodies, law enforcement agencies and other third parties. The responsibility for making these reports lies with senior managers within the Agency.

Quantification of Incidents

A method of data collection should be employed to track all incidents. This should include some type of historical database of past incidents and their resolutions. The incidents should be analyzed by type, severity, cost, and volume to determine what the actual impacts may be to the organization. Depending on the results of the analysis, data points may help identify additional controls that may be required to limit future exposure to the organization.

Agencies should regularly analyze incident logs to understand and identify future methods of prevention.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

6.3.2 Reporting Security Weaknesses

REPORTING SECURITY WEAKNESSES	
POLICY NUMBER: **6.3.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To heighten security awareness among the employees of each State of Maine Agency. It is the responsibility of each employee to safeguard information, report breeches and threats to all of the information processing systems. It is the responsibility of each organization to inform all users of the policy and process.

SCOPE

All State of Maine Agencies, their employees and third parties that are accessing information processing and communication systems.

POLICY

Each Agency shall develop a procedure for users to report threats and vulnerabilities to the security of information systems.

GUIDELINES

Agency Responsibilities

Instill a sense of urgency at the user level to report security weaknesses and threats, to all information processing and communications systems, to the designated security administrator. Users must be trained to be aware of vulnerabilities and understand the potential relationships of past incidents.

User Responsibilities

All users are expected to remain vigilant for possible fraudulent activities. Users should note and report observed or suspected security weaknesses to information technology systems and services. Users should not try to emulate the security breach or attempt to prove the threat as a test.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

6.3.3 Disciplinary Process

DISCIPLINARY PROCESS	
POLICY NUMBER: **6.3.3**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To ensure that a disciplinary process is in place to deter employees who disregard security procedures. In the event that disciplinary actions are necessary, a process will be in place that will be followed to ensure correct and fair treatment of perpetrators.

SCOPE

All State of Maine Agencies, employees and third parties that have access to information contained in the State of Maine systems.

POLICY

State and Agency-specific disciplinary procedures will be followed for users who violate information technology security policies, standards and procedures.

GUIDELINES

Disciplinary Process

A formal disciplinary process should be followed to deter and discipline employees, contractors, or vendors who have violated the organizational security policies and procedures. The process will be consistent with labor relations contracts and should ensure correct, fair treatment for employees or contractors that are suspected of committing serious and persistent breaches of security. Local law enforcement agencies should be involved, as appropriate.

Vendor Service Agreements

Vendors and contractors who provide services to the state must agree to follow the applicable security policies and procedures of the agencies for which they work. Third-party agreements should include written assurances from the vendor that they will comply with State and Agency policies and procedures, and include disciplinary action to employees of contractors who disregard security procedures.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

7. Physical and Environmental Security

7.1 Secure Areas

7.1.1 Physical Security Perimeter

PHYSICAL SECURITY PERIMETER	
POLICY NUMBER: **7.1.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To ensure that agencies take appropriate measures designed to safeguard the physical perimeter of Agency facilities that house State information systems.

SCOPE

All agencies of the State of Maine that have responsibility for facilities that physically house State of Maine information technology systems.

POLICY

> *Agencies will ensure procedures and measures are in place to prevent and detect unauthorized access or damage to facilities that contain State information systems.*

GUIDELINES

All State agencies that house information processing facilities should clearly identify the perimeter of the facility and perform a risk analysis to assess its physical security. Appropriate security controls should be applied to reduce the level of risk that has been identified. Such controls include:

➢ Physical facilities should include a structure that prevents external visual and audio observation and complies with all local building codes for structural stability (external walls, internal walls, ceilings, and doors). Walls surrounding sensitive areas of the facility should be extended from true floor to true ceiling. This height should prevent unauthorized entry and minimize environmental contamination such as that caused by fires and floods. Appropriate control mechanisms (e.g., locks, alarms, and bars.) should be applied to prevent unauthorized access.

➢ Information processing facilities should be equipped with fire, water, and physical intrusion alarm systems that automatically alert the staff to take immediate action.

➢ Information processing facilities should be equipped with doors that automatically close immediately after they have been opened. These doors should set off an audible alarm when they have been kept open beyond a certain period of time.

➢ All fire doors should be equipped with crash bars that allow occupants to quickly exit in the event of an emergency but also set off a loud alarm when the doors are opened.

➢ Sections of the facilities that house computer or communication equipment or provide access to input or output deliveries should be restricted with additional controls (see Section 7.1.2).

Confidential Location of Sensitive Information Processing Centers

The physical location of sensitive information processing facilities should be confidential and disclosed only to those having need-to-know approval. No signs should indicate the location of sensitive information processing facilities. Directories and internal telephone books that identify locations of sensitive information processing facilities should not be readily accessible by the

public.

Physical Intrusion Alarms

Unoccupied areas that house information processing facilities should be equipped with physical intrusion alarm systems. When activated, these systems should automatically alert appropriate personnel.

Location of Printers, Copiers, and Fax Machines

To prevent unauthorized duplication and transmission of sensitive information, all printers, copiers, and fax machines should be located in secured areas, not accessible to the public.

AUTHORITY, ENFORCEMENT, AND EXCEPTIONS (see Sections 1.2, 1.3, and 1.4)

TERMS AND DEFINITIONS (see Section 2)

7.1.2 Physical Entry Controls

PHYSICAL ENTRY CONTROLS	
POLICY NUMBER: **7.1.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE
To provide guidance in the protection of restricted areas using control technologies to prevent unauthorized access attempts.

SCOPE

All areas within Agency facilities that requires restricted access due to the presence of sensitive or critical State of Maine information systems within such area.

POLICY

Restricted areas within facilities that house sensitive or critical State of Maine information systems will utilize physical access controls designed to permit access by authorized users only.

GUIDELINES

Where possible, entry controls should identify, authenticate and monitor all access attempts to restricted information processing areas within Agency facilities.

Facility Identification

Access to any State data center, network operations center, telecommunications or other similar information processing facility should be restricted. Every person authorized to enter the

facility, including visitors, should be issued a facility identification badge that contains identifying information (such as name, photograph, and job position) and their level of building access. Badge color or some other bold identifier may be used to represent the level of access.

Badge Review

All badges should be checked prior to entry. A receptionist, desk attendant, security guard or electronic card reader that logs the identity, time, date, and access privileges of each entry attempt may do such checking.

Physical Access to Sensitive Information Areas

Access to any office, computer room, or work area that contains sensitive information should be physically restricted. Management responsible for the staff working in these areas should consult with security administration to determine the appropriate access control method (receptionists, metal key locks, magnetic card door locks, etc.).

Securing Sensitive Information in Unattended Locations

Sensitive information, either in paper or electronic form, should be protected from unauthorized access and disclosure. When such information is to be left in an unattended location, it should be placed in safes, file cabinets, or other appropriate containers and locked away. During non-working hours, desks should be cleared to prevent unauthorized access and disclosure of information.

Inspection of Luggage and Packages

Based on the nature and confidentiality of the information processed, users should be advised that all luggage (e.g., briefcases and backpacks) and packages are subject to inspection before entry is permitted.

Access Accountability

All entry logs should be secured and maintained. Users should challenge anyone not wearing an identification badge. Access rights to secure areas should be reviewed and updated regularly.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

REFERENCES
1. Data Centers Access Control Procedures -
    http://www.maine.gov/oit/oitpolicies/DataCenterAccessControlProcedures.htm

7.2 Equipment Security

7.2.1 Equipment Sites and Protection

EQUIPMENT SITES AND PROTECTION	
POLICY NUMBER: **7.2.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To reduce the risk to computer or communications equipment from environmental threats and hazards and unauthorized access.

SCOPE

All computer and communications equipment owned or managed by the State of Maine.

POLICY

Computer and communications equipment must be secured from physical and environmental threats to maintain the availability, integrity and confidentiality of information.

GUIDELINES

Production systems, including servers, firewalls, hubs, routers, and voicemail systems, should be located within a physically secured area.

Information systems and communications equipment that require additional security should be physically isolated to enhance the general level of protection.

To assure the continual service of critical production systems, management should provide security controls that alert, monitor, and log intrusions, fires, explosives, smoke, water, dust, vibrations, chemical and electrical effects, electrical supply interferences, and electromagnetic radiation.

Management should prohibit eating, drinking, and smoking in the proximity of information processing equipment, other than at the workstation.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

7.2.2 Power Supplies

POWER SUPPLIES	
POLICY NUMBER: **7.2.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To protect business critical equipment and information systems from power anomalies.

SCOPE

State of Maine information technology equipment that is deemed sufficiently critical to warrant power protection.

POLICY

> ***Continuity of power must be provided to maintain the availability of critical equipment and information systems.***

GUIDELINES

Uninterruptible power supplies (UPS) provide limited power to handle brief power interruptions and to allow time for the orderly shutdown of equipment for prolonged power outages. Because of the cost, UPS systems are normally recommended only for business critical operations. A risk assessment should be performed to determine the need for such equipment and the length of time outage protection is required. UPS equipment should be tested and checked regularly to ensure that it is functioning properly and has adequate capacity. Contingency plans of actions should be developed for cases of UPS failure.

Back-up generators should be considered when the risk assessment determines that processing must continue in the event of a prolonged power failure. Such a safeguard is especially important for facilities that support public safety. Generators should be tested regularly in accordance with the manufacturers' instructions. Fuel should be available to ensure that the generator can operate for a sufficient time to permit restoration of service or refueling.

Emergency power switches should be located near emergency exits in equipment rooms to facilitate rapid power down in case of an emergency. Emergency lighting should be provided within the facility in case of a main power failure. Lightning protection should be provided to all facilities, and lightning protection filters should be fitted to all external communications lines.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

7.2.3 Secure Disposal or Re-Use of Equipment

SECURE DISPOSAL OR RE-USE OF EQUIPMENT	
POLICY NUMBER: **7.2.3**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To protect exposure of sensitive information assets from improper data cleansing of equipment.

SCOPE

State of Maine computing or communications equipment that is disposed or re-used.

POLICY

> *Disposal of equipment shall be done in accordance with all applicable State or Federal surplus property and environmental disposal laws, regulations or policies to prevent unauthorized exposure of data.*

GUIDELINES

Disposal of Equipment and Deletion of Information

For the disposal of State of Maine computing equipment, users should follow procedures to render the information unrecoverable. An "erase" feature (e.g., putting a document in a trash can icon) is not sufficient for sensitive information because the information may still be recoverable.

Destruction of Media

Prior to disposal, defective or damaged media (floppy disks, CD's, tapes, etc.) containing sensitive information should be destroyed so as to render the information unrecoverable. All hardcopy materials that contain sensitive information should be shredded.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

8. Communications and Operations Management

8.1 Operational Procedures and Responsibilities

8.1.1 Documentation of Operating Procedures

DOCUMENTATION OF OPERATING PROCEDURES	
POLICY NUMBER: **8.1.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To ensure the secure operation of information processing facilities for the State of Maine through the documentation and maintenance of operating procedures.

SCOPE

All State of Maine information processing and communication facilities. This policy addresses the definition, documentation, and maintenance of the operating procedures for such systems.

POLICY

> *Operating procedures and responsibilities for all State of Maine information processing facilities will be formally authorized, documented, and maintained.*

GUIDELINES

Functional Documentation

Operating procedures for State information processing systems should be documented and approved by senior executive level management. These procedures should provide detailed directions for the execution of each job and should include:
- Instructions for handling and processing information.
- Scheduling requirements, including definitions of start/stop times and interdependencies.
- Instructions for dealing with exceptions or errors that may arise during job execution.
- Technical support contact information for trouble resolution.
- Special handling instructions on data processing output, to include disposal of output from failed jobs.
- Restart and recovery procedures for system failures.
- Security procedures and incident response plans.
- Disaster recovery procedures.
- Access approval methods.

System Maintenance Procedures

Documentation procedures should be prepared for the typical system maintenance activities associated with information processing and communications facilities. Such procedures may include:
- System start-up and close-down.
- System back-up.
- Equipment maintenance procedures and time windows.
- Computer room management and safety.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

8.1.2 Operational Change Control

OPERATIONAL CHANGE CONTROL	
POLICY NUMBER: **8.1.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To implement formal change management control procedures to protect State of Maine

information systems and services.

SCOPE

State of Maine information processing and communication facilities (e.g. Data Centers, Network Operations Centers). This policy addresses the definition and documentation of State information systems change management control procedures.

POLICY

> *Changes to all information processing facilities, systems, software, or procedures will be strictly controlled according to formal change management procedures.*

GUIDELINES

Change Management Controls

Formal management responsibilities and procedures must be implemented to ensure satisfactory control of all changes to information processing systems, software, and procedures. To reduce risk of system or security failure, the following controls should be considered:
  - ➢ Identification and recording of all significant changes in an audit log.
  - ➢ Assessment of the potential impact of such changes.
  - ➢ Formal approval procedure for proposed changes.
  - ➢ Communication of change details to all relevant persons.
  - ➢ Procedure for aborting and recovering from unsuccessful changes.
  - ➢ Build awareness of the importance of change management into system lifecycles.
  - ➢ Integration of operational and application change control procedures, wherever practical.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

REFERENCES
  1. Change Management Standard - http://www.maine.gov/oit/oitpolicies/ChangeManagementStandard.htm

8.1.3 Incident Management Procedures

INCIDENT MANAGEMENT PROCEDURES	
POLICY NUMBER: **8.1.3**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To establish response procedures to ensure the quick, orderly, and effective handling of security incidents.

SCOPE

This policy addresses the definition and documentation of security incident management procedures for such systems and services.

POLICY

> *Security incident management procedures will be established within each Agency to ensure quick, orderly, and effective responses to security incidents (as referenced in Section 6.3).*

GUIDELINES

Types of Security Incidents

Potential types of security incidents that should be covered in management procedures include:
- Breaches of confidentiality.
- Denial of service.
- Detection of network probing.
- Detection of virus or Trojan Horse activity.
- Errors due to incomplete or inaccurate data.
- Outgoing network traffic not associated with typical business processing.
- Repeated attempts of unauthorized access.
- Repeated attempts to email to unknown internal accounts.
- System activity not related to typical business processing.
- System failures and loss of service.

Procedure Provisions

Specific provisions of the incident management procedures should include:
- Contingency plans for the quick recovery of systems or services.
- Identification, analysis, and documentation of the cause of the incident.
- Planning and implementation of remedial solutions to prevent incident recurrence.
- Collection of audit trails and other similar evidence for problem analysis, compensation negotiations with suppliers, and incident follow up.
- Communication with others affected by or involved in the incident.
- Reporting of the incident to proper authorities.
- Forensics, including evidence identification and collection plans.
- System isolation plans.
- Management and law enforcement notification policy and procedure (chain of command, human resources, building security, access administration, etc.).

Recovery Procedures

Security incident recovery actions should be controlled to ensure that:
- Only clearly identified and authorized staff be allowed access to live systems and data .
- All emergency actions are documented in detail.
- Recovery procedures are promptly reported to management.

> ➢ The integrity of business systems is confirmed with minimal delay.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

8.1.4 Separation of Development and Operational Facilities

SEPARATION OF DEVELOPMENT AND OPERATIONAL FACILITIES	
POLICY NUMBER: **8.1.4**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To require the separation of operational, development, and test computing environments to reduce the risk of unauthorized access or accidental changes to operational software or data.

SCOPE

All State of Maine information processing and communication facilities. This policy addresses procedures that define the separation of State computing environments.

POLICY

> *Operational computing environments will be separated from development and test computing environments to reduce the risk of one environment adversely affecting another.*

GUIDELINES

Level of Separation

Separation between operational, development, and test systems should be maintained to reduce the risk of unauthorized changes or access. To operate properly, each type of computing system requires a known and stable environment. The opportunity for interference among development, testing, and operational systems must be prevented. The following should be considered:

> ➢ Run development and operational software on different computer processors, in different domains, or in different directories.
> ➢ Separate development and testing activities from production activities.
> ➢ Prevent the access of software development utilities from operational systems, when not required.
> ➢ Avoid using the same log-on procedures, passwords, and display menus for both operational and test systems, to reduce the risk of accidental log-on and other errors.
> ➢ Implement controls to ensure that administrative passwords for operational systems are closely monitored and controlled.
> ➢ Define and document the procedures for transferring software from development to operational status. Such transfers should require management approval.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

8.1.5 External Facilities Management

EXTERNAL FACILITIES MANAGEMENT	
POLICY NUMBER: **8.1.5**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To reduce security exposure and prevent compromise, damage, or loss of data when external contractors provide information processing facilities for State systems or services.

SCOPE

Contracted services for information-processing facilities that are entrusted with State of Maine information assets. This policy defines controls for the security of external computing environments provided for State information systems and services.

POLICY

Contractual controls consistent with the State of Maine IT Security Policy will be established to reduce security risks created when external contractors are utilized to provide information processing facilities.

GUIDELINES

Considerations for the Use of External Facilities

The use of external provider information processing facilities introduces potential security exposures and requires that special precautions be incorporated into contracts for service. Specific risks should be identified in advance and appropriate controls should be agreed upon with the contractor (see Section 4.2 and 4.3 for guidance on third party contracts). The following issues should be addressed:

- ➢ Identify sensitive or critical applications that should be retained in-house.
- ➢ Obtain approval of business application owners to utilize external facilities.
- ➢ Consider business continuity plan implications.
- ➢ Specify security standards and compliance measurement processes.
- ➢ Define specific responsibilities and procedures to effectively monitor all relevant security activities.
- ➢ Specify background checks and other techniques that will be used to screen vendor personnel, and require confirmation that background checks have been successfully completed.
- ➢ Define responsibilities and procedures for reporting and handling security incidents.
- ➢ Define the security parameters for communications and data to the external site.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

REFERENCES
1. Remote Hosting Policy - http://www.maine.gov/oit/oitpolicies/RemoteHostingPolicy.htm

8.2 System Planning and Acceptance

8.2.1 Capacity Planning

CAPACITY PLANNING	
POLICY NUMBER: **8.2.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To ensure the proper management of capacity planning to meet current and future information system requirements so as to minimize the risk of failure due to inadequate system resources.

SCOPE

All State of Maine information processing and communication facilities. This policy addresses the ongoing requirement for capacity planning for all State information systems and services.

POLICY

System capacity requirements will be monitored and usage projected to ensure the continual availability of adequate processing power, bandwidth, and storage.

GUIDELINES

Monitoring and Projecting Capacity Requirements

The continually changing demands for information systems processing power, bandwidth, and storage require regular monitoring of current State system usage. Future capacity requirements should also be projected. Key system resources include processors, main storage, file storage, printers, and communications systems.

Information system managers should monitor resources to identify usage trends and changes to specific applications or systems. Growth in system capacities should be projected to support new business requirements and to plan new applications. With proper monitoring and projecting, managers can identify and avoid potential capacity bottlenecks that threaten system security or operation.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

8.2.2 System Acceptance

SYSTEM ACCEPTANCE	
POLICY NUMBER: **8.2.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To reduce the risk of system failure due to inadequate testing and validation acceptance of new or upgraded information systems.

SCOPE

All State of Maine information processing and communication facilities. This policy addresses the requirement for system acceptance testing of all new or upgraded State information systems and services.

POLICY

System acceptance criteria for all new information systems and system upgrades must be defined, documented, and utilized to minimize risk of system failure.

GUIDELINES

Acceptance Controls

Prior to the implementation of new or upgraded information systems, care should be taken to ensure that all requirements for acceptance have been met. Criteria should be clearly defined, documented, and tested, with consideration given to the following controls:
  - Approved security controls.
  - Business continuity preparations.
  - Error recovery, restart, and contingency plans and procedures.
  - Manual operating procedures.
  - Operation training on use of the new system.
  - Penetration testing.
  - Projected performance and capacity requirements.
  - Standardized routine operating procedures.
  - User verification of proper operational performance.
  - Verification of the non-impact of the new system on existing systems and on overall organizational security.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

REFERENCES
1. Deployment Certification Policy for Major Application Projects -
   http://www.maine.gov/oit/oitpolicies/DeployCertPolicy.htm

8.3 Protection Against Malicious Software

8.3.1 Controls Against Malicious Software

CONTROLS AGAINST MALICIOUS SOFTWARE	
POLICY NUMBER: **8.3.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To protect the integrity of information systems and software through requirements for the prevention and detection of malicious software.

SCOPE

All State of Maine information processing and communication facilities. This policy addresses the requirement for security awareness and appropriate controls to protect all State information systems and services against the introduction of malicious software.

POLICY

Security awareness, prevention, and detection controls will be utilized to protect information systems and services against malicious software.

GUIDELINES

Malicious Software Controls

Unless proper control precautions are taken, information systems are vulnerable to the introduction of malicious software such as computer viruses, network worms, Trojan horses, and logic bombs. Appropriate security procedures should be utilized to ensure that users are aware of the dangers of unauthorized or malicious software. In addition, special controls that detect or prevent the introduction of malicious software should be introduced. Protection should be based on awareness, change management, and system access controls, such as the following:
  ➢ A formal policy requiring compliance with software licenses and prohibiting use of unauthorized software.
  ➢ A formal policy protecting against the risks of obtaining software files from external sources.
  ➢ Installation, update, and consistent use of anti-virus software (especially on personal computers and network file servers) to scan systems and media as a precautionary measure.
  ➢ Requirements for regular reviews of critical system data content to identify unapproved or unauthorized files.

> ➢ Requirement to check any file received from an unknown or distrusted source for viruses before use. Requirement to check all electronic mail attachments and file downloads for malicious software before use.
> ➢ System management training on establishing virus protection, reporting incidents, and recovering from virus attacks.
> ➢ Business continuity plans and arrangements for recovering from virus attacks.
> ➢ Procedures to ensure that all communications related to malicious software, such as warnings or bulletins, are accurate and informative.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

8.4 Housekeeping

8.4.1 Information Back-Up

INFORMATION BACK-UP	
POLICY NUMBER: **8.4.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To ensure that back-up copies of essential electronically-stored business data are routinely created and properly stored and that procedures and facilities for restoring such data are prepared and tested.

SCOPE

All State of Maine information processing and communication facilities. This policy addresses the requirement for regular back-ups and preparation for restoration of essential State information systems and services.

POLICY

> *Back-ups of all essential State of Maine electronically-stored business data must be routinely created and properly stored to ensure prompt restoration.*

GUIDELINES

Back-up Considerations

Routine procedures should be followed to implement Agency back-up strategies. In addition, system facilities should be tested to ensure that all essential business data could be recovered following a disaster or system failure. The following controls should be considered:
> ➢ A current, complete, minimum level back up, together with documented procedures and

accurate records of the back-up copies, should be stored at a remote location, a sufficient distance from the main site, to escape damage from disaster.

➢ At least three cycles of backups should be retained for critical business applications.
➢ The retention period for essential data and the special requirements for permanent archives should be defined as required.
➢ Back-up information should be stored in a physically and environmentally protected site. The same controls applied to media at the main site should be applied to media stored at the back-up site.
➢ Back-up media should be tested regularly to ensure that they can be reliably restored.
➢ Regular testing of the restoration procedures should ensure that the procedures are appropriate, the restoration systems are adequate, and the restoration process can be completed within the time allotted in the recovery procedures.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

8.4.2 Activity Logs

ACTIVITY LOGS	
POLICY NUMBER: **8.4.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To require the maintenance of activity logs for State of Maine information systems by the operational staff.

SCOPE

All State of Maine information processing and communication facilities. This policy addresses the requirement for operational logs of all activities related to State information systems and services.

POLICY

Appropriate log(s) of activities involving State of Maine information systems and services will be maintained and reviewed.

GUIDELINES

Operator Log Requirements

Logs should be maintained and securely stored. These logs should be subject to regular, independent reviews and should include such appropriate information as:
➢ Start and finish date and time for system activity.
➢ System errors and corrective actions taken.

➢ Confirmation of proper handling of media and output.
➢ Name of the person making the log entry.

Automated Logs

Automated logging should be used whenever possible for:
➢ System utilization.
➢ System errors and corrective actions taken (especially automated error recovery).
➢ Communication session statistics.
➢ Successful and unsuccessful logins.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

REFERENCES
1. **(EISD-SD-2008.01) Security Configuration for Standard Desktop Image -**
   http://inet.state.me.us/oit/services/CoreTechnology/security/Security%20Directives/EISD%20Security%20Directive%20-%20EISD-SD-2008%2001.doc

8.4.3 Fault Logging

FAULT LOGGING	
POLICY NUMBER: **8.4.3**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To require that all faults involving State of Maine information systems and services be properly logged and reported and that appropriate action is taken to correct them.

SCOPE

All State of Maine information processing and communication. This policy addresses the requirement for fault logs related to State information systems and services.

POLICY

All faults involving State of Maine information systems and services must be logged, reported, and appropriate action taken.

GUIDELINES

Manual Fault Logging

Computer operations personnel who monitor system operations should maintain a fault log. This log ensures that complete, accurate records of all system and service faults are maintained and that all faults are properly handled. The log should include:
➢ Date and time of log entry.

➢ Description of fault and corrective actions taken.
➢ Name of the person making the log entry.
➢ Review and confirmation of proper handling of fault.
➢ Review of corrective measures to ensure that controls have not been compromised.

Automated Fault Logging

Where computer or network operations can be monitored by automated means, the automated fault logging capability should be enabled. This log ensures that complete, accurate records of all system and service faults are maintained and that all faults are properly handled. The log should include:
➢ Date and time of log entry.
➢ Description of fault and corrective actions taken (especially any automated recovery).
➢ Security exceptions or intrusion alerts.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

8.5 Network Management

8.5.1 Network Controls

NETWORK CONTROLS	
POLICY NUMBER: **8.5.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

➢ To require controls for the security of data on networks.
➢ To protect connected services from unauthorized access.

SCOPE

This policy addresses the requirement for controls to safeguard information on all State of Maine information systems networks and to protect the supporting infrastructure of such networks.

POLICY

Agencies must establish operational controls and safeguards to ensure the security of information systems and the protection of the supporting network infrastructure. The Office of Information Technology Wide Area Network (WAN) policy will address security of the WAN and its supporting infrastructure. Agency network infrastructure that impacts the WAN will be coordinated with the Office of Information Technology.

GUIDELINES

Network Security

To achieve and maintain security on computer networks, a range of controls must be utilized. The common objective of these controls should be to protect all information and to protect all connected services from unauthorized access. Security management of networks may span organizational boundaries and may involve protecting sensitive data passing over public networks. The following controls should be considered:
 ➢ Operational responsibilities for networks and for computer operations should be separated, where appropriate.
 ➢ Remote equipment management responsibilities should be established.
 ➢ Special controls should be established to protect data passing over public networks and to protect connected systems.
 ➢ Network management tools and procedures should be used to ensure that controls are consistently applied and that services are optimized.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

REFERENCES
 1. Telecommunications Facilities and Wiring Specifications - http://www.maine.gov/oit/oitpolicies/WireSpec5_1_08_05.htm

8.6 Media Handling and Security

8.6.1 Disposal of Media

DISPOSAL OF MEDIA	
POLICY NUMBER: **8.6.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To require the secure disposal of State computer media

SCOPE

State of Maine removable computer media (e.g., tapes, disks, cassettes, CDs, printed reports and operational logs). This policy addresses the requirement for the proper disposal of State information contained in removable media.

POLICY

When no longer required, the contents of removable media will be disposed of, permanently destroyed or rendered unrecoverable in accordance with applicable State, Federal or Agency record retention requirements (see also Section 5).

GUIDELINES

Secure Media Disposal

When media is worn, damaged or otherwise no longer required, it should be disposed of in a secure manner. To prevent the compromise of sensitive information through careless or inadequate disposal of computer media, formal procedures should be established for secure media disposal. The following considerations should be included:
- ➢ Items which may require secure disposal include paper documents, recordings, output reports, magnetic tapes, printers, faxes, copiers, removable disks or cassettes, optical storage media, program listings, test data, and system documentation.
- ➢ Media containing sensitive information should be disposed of by secure incineration or shredding.
- ➢ If the magnetic or optical media is to be reused, it should be completely emptied of data and prepared by special software designed to securely erase and/or reformat the media.
- ➢ Care should be taken when selecting a media disposal contractor to ensure adequate security control and experience.
- ➢ A log should be maintained of the disposal of all sensitive items so as to provide an audit trail.
- ➢ Consideration should be given to the extra risks associated with accumulating a large volume of media prior to disposal. In large quantities, it may be more difficult to detect missing items.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

REFERENCES

8.6.2 Information Handling Procedures

INFORMATION HANDLING PROCEDURES	
POLICY NUMBER: **8.6.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To require procedures for the secure handling and storage of all State of Maine information

SCOPE

State of Maine information handled or stored by information processing systems or services. This policy addresses the requirement for proper handling procedures for all State information.

POLICY

Internal procedures must be established for the secure handling and storage of all electronically stored information that is owned or controlled by an Agency.

GUIDELINES

Secure Information Handling

Procedures for the secure handling and storage of State information are required to protect that information from unauthorized disclosure or misuse. Such procedures should be consistent with the type of information. The following controls should be considered:

➢ Include handling of documents, computing systems, networks, mobile users, postal services, electronic mail, voice mail, voice communications, fax machines, multimedia,, and sensitive items (e.g., checks and invoices).
➢ Describe methods of handling and storing media.
➢ Use access restrictions to identify unauthorized personnel.
➢ Maintain formal records of the recipients of data.
➢ Store media in accordance with manufacturers' specifications.
➢ Restrict distribution of information.
➢ Indicate the authorized recipient of all copies of data.
➢ Review distribution lists and verify authorized recipients at regular intervals.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

8.6.3 Security of Operational System Documentation

SECURITY OF OPERATIONAL SYSTEM DOCUMENTATION	
POLICY NUMBER: **8.6.3**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To require the implementation of security controls to protect all State of Maine operational system documentation from unauthorized access.

SCOPE

Operational system documentation for State of Maine information systems or services (e.g. Network diagrams, router configuration, firewall rule sets, etc.). This policy addresses the requirement for proper security procedures for such operational system documentation.

POLICY

Operational system documentation for State of Maine information systems must be protected from unauthorized access.

GUIDELINES

Operational System Documentation Security

Operational System Documentation means those operational manuals, tables, access control lists, or other documentation that contain sensitive information such as the descriptions of application processes, procedures, data structures, addressing schemes, and authorization processes which if divulged could compromise the security of the systems referenced within such documentation.

Since the operational system documentation for State of Maine information systems may contain sensitive information, it must be protected from unauthorized access. The following controls should be considered:

- ➢ Store system documentation in a manner that is consistent with its classification.
- ➢ Restrict the access list for system documentation to the minimum authorized by the application owner.
- ➢ Protect system documentation on or accessed over a public network.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

8.7 Exchanges of Information and Software

8.7.1 Information and Software Exchange Agreements

INFORMATION AND SOFTWARE EXCHANGE AGREEMENTS	
POLICY NUMBER: **8.7.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance in creating software exchange agreements. Such agreements are intended to prevent loss, modification or misuse of information shared between organizations.

SCOPE

This policy covers agreements for the sharing of information between agencies of the State of Maine and external (i.e. third party) organizations.

POLICY

Agreements must be developed and implemented for the exchange of information between Agencies within the State of Maine and other external entities to extend appropriate security controls (see also Section 4).

GUIDELINES

The exchange of information with other organizations should be based on a formal agreement that specifies the conditions and handling of the information (e.g. Non-disclosure agreements).

The agreement should exist whether the information is in electronic or physical form. The content of the agreement will vary depending on the reason for the exchange. Depending on the nature and scope of the exchange, the security components of the exchange agreement should contain provisions addressing one or more of the following items:

➢ Management responsibilities for controlling and notifying of transmission, dispatch and receipt.
➢ Procedures for notifying sender of transmission dispatch and receipt.
➢ Minimum technical standards for packaging and transmission.
➢ Courier identification standards.
➢ Responsibilities and liabilities in the event of lost data.
➢ Use of an agreed labeling system for critical or sensitive data ensuring that the meaning of the labels are immediately understood and protected appropriately.
➢ Information and software ownership and responsibilities for data protection, software copyright compliance and similar considerations (see also section 12.1.1).
➢ Any special controls that may be required to protect sensitive items, such as cryptographic keys.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

8.7.2 Electronic Commerce Security

ELECTRONIC COMMERCE SECURITY	
POLICY NUMBER: **8.7.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance for the use of electronic forms of data interchange involving various forms of commerce.

SCOPE

State of Maine information processing and communication facilities

POLICY

State of Maine information that is accessed via electronic commerce activities must have security controls implemented based on a risk assessment and an information classification scheme.

GUIDELINES

Electronic commerce can involve various types of communications, such as EDI, electronic mail and Internet based web servers. Each State Agency should review the sensitivity of the type(s) of data to be exchanged. The result of this analysis should be used to determine the appropriate

security controls necessary to protect the confidentiality, integrity, and availability of the information being exchanged through the electronic commerce process.

The following security risks should be considered in the design of all e-commerce applications:
- ➢ Vulnerability of messages to unauthorized access or modification or potential exposure to denial of service attacks.
- ➢ Vulnerability to error, e.g. incorrect addressing or misdirection, and the general reliability and availability of the service.
- ➢ Impact of a change of communications media on business process, e.g. the effect of increased speed of dispatch or the effect of sending formal messages from person to person rather than company to company.
- ➢ Legal considerations, such as potential need for proof of origin, dispatch, delivery and acceptance.
- ➢ Vulnerability of the application to invalid data (i.e. buffer overflows).

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

8.7.3 Security of Electronic Mail

SECURITY OF ELECTRONIC MAIL	
POLICY NUMBER: **8.7.3**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide coordination and guidance on the establishment, administration and use of email systems, and to ensure the effective and safe use of email services in State government. The use of email for conducting State business should be based on business management decisions regarding the appropriateness of the medium.

SCOPE

All Agencies of the State of Maine.

POLICY

The Office of Information Technology will be solely responsible for the establishment, maintenance, and administration of an enterprise-wide email application for the State of Maine. Agencies will establish acceptable use policies for the use of electronic mail, which will include inspection or review by Agency management to comply with State and Federal regulations as well as any applicable Agency policies.

GUIDELINES

The Office of Information Technology serves as the e-mail portal for State e-mail services and is

responsible for providing support for the email application standard adopted by the State of Maine. Procedures for the establishment, administration and acceptable use of State email resources should, at a minimum, address the following issues:

➢ Attacks on electronic mail, e.g. viruses, interception, user identification, defensive systems.
➢ Protection of electronic mail attachments using such techniques as Filtering, Stripping, or Store and Forward.
➢ Avoidance of e-mail platforms serving as open mail relays.
➢ Restrictions for the use of email involving defamatory, harassing, or other forms of illegal or injurious electronic mail.
➢ Use of cryptographic techniques to protect the confidentiality and integrity of electronic messages.
➢ Retention of messages.
➢ Proper handling of messages in which sender cannot be authenticated.
➢ Agreements for State employees for acceptable use and inspection of emails, without the expectation of privacy.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

8.7.4 Publicly Available Systems

PUBLICLY AVAILABLE SYSTEMS	
POLICY NUMBER: **8.7.4**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance for the use of publicly available methods of access, such as the Internet, to State information resources.

SCOPE

All agencies of the State of Maine.

POLICY

Public access to State electronic information resources must provide desired services in accordance with safeguards to protect State resources.

GUIDELINES

The dissemination methods for State information classified as "public" should have, at a minimum, protection from unauthorized modification and denial of service attacks.

Consideration of security controls that should be applied to publicly available systems should

include the following:
- ➢ Information to be disseminated is classified in compliance with current data protection legislation.
- ➢ Any information input to, and processed by a public system, such as a request form, comment form, questionnaire, etc., will be processed completely, accurately and in a timely manner.
- ➢ Sensitive information will be protected during the collection process and when stored.
- ➢ Access to the public system does not allow unauthorized access to networks to which it is connected State information classified as other than public should not reside on systems where public information is being served. Information to be made available to restricted groups, such as employees, should be protected by appropriate security mechanisms.

Web Servers

Where e-commerce involves using the Internet, some form of periodic penetration testing or other security assessment should be performed to ensure that security has not been compromised. Where web servers are involved, the testing should include a complete analysis of the web site by a third party. At a minimum, the analysis should include the following:
- ➢ External testing.
- ➢ Web site map.
- ➢ Hypertext Link integrity test.
- ➢ Common Gateway Interface (CGI) testing.
- ➢ Identification of Server.
- ➢ Identification of all responding ports on Web server IP address.
- ➢ Testing for known subversions based on server technology.
- ➢ Complete mapping of observable IP network from the Internet.
- ➢ Memory bounding and exception handling.
- ➢ Internal Testing.
- ➢ Security policy audit.
- ➢ Change Controls.
- ➢ User Accounts.
- ➢ Backup and Recovery.
- ➢ Intrusion Detection.
- ➢ Detection of unauthorized changes.
- ➢ DMZ penetration testing.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

9. Access Control

9.1 Business Requirement for Access Control

9.1.1 Access Control Policy

ACCESS CONTROL POLICY	
POLICY NUMBER: **9.1.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To define access controls to information systems and resources for the State of Maine. Information access and State computing processes should be controlled on the basis of State business and applicable security policies.

SCOPE

All agencies of the State of Maine. Users have responsibility to safeguard access to State resources that has been entrusted to them.

POLICY

Access to State information systems and computing resources will be based on each user's access privileges. Access privileges shall be granted on the basis of specific business need (i.e. a "need to know" basis). Access Controls must ensure that even legitimate users cannot access stored information unless they are authorized to do so.

GUIDELINES

System Access Controls

All sensitive computer-resident information should be protected via access controls to ensure that it is not improperly disclosed, modified, deleted, or rendered unavailable. Access control procedures should not only control access based on the need to know, they should also log which users accessed the sensitive data.

Need to Know

Information should be disclosed only to those people who have a legitimate business need for the information ("need to know").

Access Approval Process

A supervisor and/or manager should initiate the access approval process, and the privileges granted should remain in effect only until the employee's job changes or the employee leaves the employer. When either of these events takes place, the manager and/or supervisor should immediately notify the appropriate access administration. All contractors, consultants, temporaries, outsourcing firms, etc. should also go through a similar access control request and authorization process. The privileges of these contracted resources should be immediately revoked by access administration at the conclusion of the assignment for which they were granted access.

Granting Access Authority

The authority to grant access to State of Maine information should be provided only by the owner of the information or their delegate.

Default Access Control Privileges

Default access privileges should be set to "deny-all" prior to any specific permissions being granted.

Custom Application Development

All custom-developed software intended to create or modify State of Maine information should have a formal written specification. This specification should include discussion of both security risks and controls (including access control systems and response plans for security events).

Restricted and Monitored Use of Systems Software Utilities

Access to systems software utilities should be restricted to authorized users. For production computing resources, a change control process should be in place (See Section 10).

Dissemination of Information

Unless it has specifically been classified as public, all State of Maine information should be protected from disclosure. Only the information owners or their delegate may grant permission to disseminate the information. If non-public information is compromised or suspected of being compromised, the information owner and the appropriate security administration should be notified immediately.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

9.2 User Access Management

9.2.1 Access Authorization

ACCESS AUTHORIZATION	
POLICY NUMBER: **9.2.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To manage the allocation of user access rights in accessing State of Maine Information Systems and Resources.

SCOPE

All stages in the life cycle of user access, from the initial registration of new users to the final de-registration of users who no longer require access to State of Maine information systems and resources.

POLICY

> *User access to all systems will be authorized by the Agency owner of the system.*

GUIDELINES

User Identification and Privileges Need Explicit Written Approvals

User-IDs may be granted to specific users only when approved in advance by the user's immediate manager and/or supervisor. Prior to being granted to users, business application system privileges should be approved by the information owner. Without specific written approval from user's management, administrators should not grant system privileges to any user. All users should be positively identified prior to being able to use any multi-user computer or communications system resources.

User Access to Information Systems and Resources

All users should have their identity verified with a user-ID and a secret password issued by the appropriate authority prior to being permitted to use State computers and network resources. State employees that need access to information systems and/or resources to perform their job role should be granted appropriate access based on approval. System access should be provided via job profiles or by special request directed to the owner of the information or resource.

Users Responsibility for All Activities Involving Personal User-IDs

Users are responsible for all activity performed with their personal user-IDs. User-IDs should not be utilized by anyone but the individuals to whom they have been issued. Users should not allow others to perform any activity with their user-IDs. Similarly, users should not perform any activity with IDs belonging to other users. Users should sign (physically or electronically) an agreement indicating that the user understands the conditions of access prior to being given a user-ID that allows access to State systems. Users should be given a statement describing their access authorities.

Third Party Access to State of Maine Systems Requires Signed Contract

Before any third party is given access to State systems, a contract defining the terms and conditions of such access should have been signed by a responsible manager at the third party organization. Both the security administration and the purchasing authority should approve these terms and conditions. All State information systems privileges should be promptly terminated at the time that a third party agent ceases to provide services to the State.

Periodic Review of Access Privileges

The user's immediate manager and/or supervisor should periodically reevaluate the system privileges granted to a user. This reevaluation involves a determination of whether currently enabled system privileges are still needed to perform the user's current job duties.

User Authentication

All production information system user-IDs should have a linked password or a stronger mechanism (such as a dynamic password token) to ensure that only the authorized user is able to utilize the user-ID. Users are responsible for all activity that takes place with their user-ID and password (or other authentication mechanism). Users should immediately change their password if they suspect that it has been discovered or used by another. Likewise, users should notify the appropriate security administrator if other access control mechanisms are broken or if they suspect that these mechanisms have been compromised.

Unique User-IDs

Users should be assigned their own unique user-ID. This user-ID should be decommissioned when a user terminates employment with the State of Maine. User-IDs and related passwords should not be shared with any other individuals. User-IDs should be linked to specific people, and should not be associated with computer terminals, departments, or job titles. Anonymous user-IDs (such as "guest") should not be allowed unless approved in advance by the appropriate access administration.

Changes in User Duties

Management should promptly report all significant changes in end-user duties or employment status to the appropriate security administrator handling the user-IDs of the affected persons.

Access Privileges Cease When Workers Terminate

All State information systems privileges should be promptly terminated at the time that a worker ceases to provide services to the State of Maine.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

9.2.2 Privilege Management

PRIVILEGE MANAGEMENT	
POLICY NUMBER: **9.2.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To ensure management of user access privileges for State of Maine information systems.

SCOPE

Control of user privileges for State Agencies. This will enable the State to prevent unauthorized access to sensitive information from multi-user systems.

POLICY

> *Agencies must establish procedures to modify the functionality, connectivity, and services supported by information systems that restrict users' privileges based on requirements of their job function.*

GUIDELINES

Allocation of Privileges for Users and State System Resources

Users should be allocated privileges with the minimum requirement for their job function on a need-to-use basis and on an event-by-event basis. Privileges associated with State of Maine system resources, e.g. operating system, database management system, applications, and the categories of staff should be identified prior to allocation.

User-To-User Separation of Activities and Data

Management should define user privileges such that unauthorized users cannot gain access to, or otherwise interfere with, either the individual activities or the data of other users.

Logging and Reporting on Privileged User-ID Activity

All user-ID creation, deletion, and privilege change activity performed by systems administrators and others with privileged user-IDs should be securely logged and periodically reviewed by management.

Special Access Privileges

Special access privileges, such as the ability to examine the files of other users, should be restricted to those directly responsible for system management and/or information security.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

9.2.3 Review of User Access Rights

REVIEW OF USER ACCESS RIGHTS	
POLICY NUMBER: **9.2.3**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To maintain effective control over access to data and information services to ensure that unauthorized privileges have not been obtained.

SCOPE

Review of privileges allocated users and access control rights.

POLICY

> *Periodic log reviews of user access and privileges must be performed in order to monitor access of sensitive information.*

GUIDELINES

User Access Rights Review

User access rights should be reviewed periodically (see Section 9.2.1, *Periodic Review of Access Privileges*)

Special Privilege Access Rights Review

Authorization for special privileged access rights should be reviewed on a frequent basis by the appropriate level of management supervision.

Privilege Allocation Review

Management and security administration should conduct periodic checks on privileges granted each user to ensure that unauthorized access has not been obtained.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

9.3 User Responsibilities

9.3.1 Password Use

PASSWORD USE	
POLICY NUMBER: **9.3.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To establish a standard for creation and use of passwords, the protection of those passwords, and the frequency of change for such passwords to prevent compromise of confidential information.

SCOPE

All personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any State of Maine facility, has access to the State of Maine network, or stores any State of Maine information.

POLICY

Passwords are a primary means to control access to systems. Users will select, employ, and manage passwords to protect against unauthorized discovery or usage.

GUIDELINES

Password Uses

Passwords are used for various purposes for State of Maine computing resources. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have support for one-time tokens (i.e., dynamic passwords which are only used once) all users should utilize strong passwords.

Password Construction

Strong passwords provide the first line of defense against improper access and compromise of confidential information. Strong passwords typically exhibit the following best practice characteristics:
  - Contain both upper and lower case characters (e.g., a-z, A-Z).
  - Have digits and special characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-
  - =\`{}[]:";'<>?,./).
  - Are at least eight alphanumeric characters long.
  - Are not words in any language, slang, dialect, jargon, etc.
  - Are not based on personal information, names of family, etc.
  - Are not to be written down or stored on-line.
  - Should be easily remembered. One way to do this is create a password based on a song title, affirmation, or other phrase. For example, the phrase might be: "This May Be One Way to Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.
  - Should never be null passwords or passwords which are the same as user ID's.

Password Protection

All system-level passwords (e.g., root, enable, Windows administration, application administration accounts, etc.) should be changed at least every 90 days. All user-level passwords

(e.g., email, web, desktop computer, application, etc.) should be changed at least every 120 days. User accounts that have system-level privileges granted through group memberships or programs should have a unique password from other accounts held by that user. Passwords should not be inserted into email messages or other forms of electronic communication.

Users should not use the same password for State of Maine accounts as for other non-State of Maine access (e.g., personal ISP account, option trading, benefits, etc.). Where possible, users should not use the same password for different State of Maine access needs. For example, a user should select one password for the Engineering systems and a separate password for IT systems. Also, a separate password should be selected to be used for operating system accounts. The exception to this is where a Single Sign-on System may control multiple systems.

Users should not share State of Maine passwords with anyone, including administrative assistants or secretaries. All passwords should be treated as sensitive, confidential information. Users should not write passwords down and store them anywhere in their office. Nor should they store passwords in a file on ANY computer system (including Personal Digital Assistants or similar devices) without encryption. Users should not use the "Remember Password" feature of applications.

If an account or password is suspected of being compromised, the incident should be reported to the appropriate access administrator and the user should change the password. Security administrators should perform periodic, random password audits via automated tools or guessing. If a password is determined during one of these scans, the user should be required to change it.

User Should Not Employ Any Automatic Log-In Actions

State of Maine information system users should refuse all offers by software and/or Internet sites to automatically login the next time that they access those resources.

Password Sharing Prohibition

Besides the authorized user, passwords should never be shared or revealed to anyone. To do so exposes the authorized user the responsibility for actions that the other party takes with the password. Temporary or "first use" passwords should be changed the first time that the authorized user accesses the system. If users need to share computer resident data, they should use approved network services or any other mechanisms that do not infringe on any policies.

Application Development

Application developers should ensure their programs contain the following security precautions:
  ➢ Applications should support authentication of individual users, not groups.
  ➢ Applications should not store passwords in clear text or in any easily reversible form.
  ➢ Applications should provide for some sort of role management, such that one user can take over the functions of another without having to know the other's password.

Use of Passwords and Pass phrases for Remote Access Users

Access to the State of Maine Networks via remote access should be controlled using either a one-time password authentication or a public/private key system with a strong pass phrase. Pass phrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the pass phrase to "unlock" the private key, the user cannot gain access.

Pass phrases are not the same as passwords. A pass phrase is a longer version of a password and is, therefore, more secure. A pass phrase is typically composed of multiple words. Because of this, a pass phrase is more secure against "dictionary attacks." A good pass phrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. All of the rules that apply to passwords apply to pass phrases.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

REFERENCES
1. **Password Policy** -
   http://inet.state.me.us/oit/services/CoreTechnology/security/Password%20Policy%20for%20Windows.htm

9.4 Network Access Control

9.4.1 Use of Network Services

USE OF NETWORK SERVICES	
POLICY NUMBER: **9.4.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To establish guidelines for access and use of networks and networked services.

SCOPE

All users in all agencies, including those users affiliated with third parties who access State agencies computer networks. The policy also applies to all computer and data communication systems owned by and/or administered by State agencies.

POLICY

Access to the State of Maine Wide Area Network and its resources, operated by the Office of Information Technology, and networks operated by other Agencies, will be strictly controlled, managed, and reviewed by the Agency responsible for the network to ensure only authorized users gain access based on the privileges granted.

GUIDELINES

The objective of these guidelines is to establish a baseline for protection of all State of Maine networking services. Control of access to both internal and external network services is necessary to ensure that all users of the networks and network services do not intentionally or unintentionally compromise the security of these networks. These guidelines will cover user and equipment authentication mechanisms, control of user access of information services and the appropriate interfaces between State of Maine network and networks owned by other entities.

Use of Network Services

➢ Users should have their identity verified with a State issued user-id and a confidential password prior to being permitted to use State Agency network connected systems.
➢ Systems that can be reached by third party networks should have appropriate access control systems approved by the Office of Information Technology (security administration).
➢ Internal networks that store sensitive information should have an authentication system approved by the Agency information technology security officer(s).
➢ In-bound connections to State systems should be protected with an approved dynamic password access control system.
➢ Agencies should refer to the Office of Information Technology WAN Policy to connect to third party systems.

User Authentication for External Connections

➢ Access to State agencies internal networks from any location should follow a management approval process.
➢ Both the owner of the information and the manager in charge of the third party's work should follow the guidelines provided and should agree to sign a compliance statement prior to establishing access.
➢ Outbound connections initiated from a State of Maine office should be routed through dial-up modem pools, Internet firewalls, and other systems expressly established to provide secure network access.
➢ Whenever a State of Maine system has approval to transmit sensitive information outside its network(s) the link should be encrypted. Such encryption should be accomplished only with systems approved by the security administrator(s).
➢ A connection that is established between any external system or network and a State of Maine internal system or network should not involve the use of shared file systems.
➢ Up-to-date virus checking programs approved by the security administration should be continuously enabled on all web servers, LAN servers, mail servers, firewalls, and networked PCs.
➢ Systems accepting remote connections from public networks such as the dial-up phone network or the Internet should include a session time-out mechanism.
➢ Login banners should be used on all State of Maine networks and computers that are directly accessible through external networks.

> ➢ All State agencies computers and networks which interface to external networks should maintain system logs that indicate the time and date, identity and activity performed by each user who gains access to these systems.
> ➢ All State of Maine networks that are connected to external networks should implement control mechanisms such as firewalls, routers, and gateways.

Node Authentication

Authentication should be applied to host systems that accept automatic connections from remote computers such as Virtual Private Networks (VPN), and Remote Access Services.

Remote Diagnostic Port Protection

Approval to enable a maintenance port on a communication device should follow a management approval process including change control. Proper restrictions and procedures should be in place to prevent an open vulnerability from an unauthorized user.

Segregation in Networks

Large networks crossing organizational boundaries should obtain separately defined logical domains, each protected with suitable security perimeters and access controls. Research and development networks should have physical or logical separation from production networks.

Intrusion Detection Systems

Intrusion detections systems should be used for at key communication segments to intercept and analyze traffic that would be disruptive to the State. These systems should be monitored and updated routinely for current patches and signatures for intrusion detection.

Network Connection Control

In-bound connections to State agencies internal networks and/or information systems from external sources should pass through an additional access control point (e.g. a firewall, gateway, or access server) before users can reach a login screen.

> ➢ For web access, all inbound applets containing active content (Sun's Java, Microsoft's Active X, Microsoft's Visual Basic scripts, Macromedia Shockwave files, etc.) should normally be blocked by a firewall. Specific exceptions should be approved through the appropriate security administrator.
> ➢ Once the configuration and permissible service of firewall, router, and access control devices have been established and set to follow specific policies these policies should not be changed without prior permission of the appropriate security administrator.
> ➢ All firewalls, routers, and access control devices used to protect State agencies internal network should run on separate dedicated computers. These computers should not serve other purposes such as act as web servers.

Network Routing Control

Proper access control lists should be applied on all communication devices (routers, firewalls, servers) to prevent the act of intentional or unintentional access to unauthorized routes into systems and network resources.

Unused ports should be disabled to prevent unauthorized connections of devices that could have the possibility of bypassing the login server.

Security of Network Services

Prior to engaging with network service providers, all documentation that describes Agency systems or systems procedures should be reviewed by the information technology security officer and/or the Agency Technology Officer to ensure that confidential information is not being inadvertently disclosed.

When a service provider is acting as a common carrier and is providing communications services to State agencies no responsibility is assumed for the disclosure of information placed on the network, and no assurances are made about the privacy of information placed on the network.

Agreements dealing with the handling of State Agency information traffic by service providers should include clear description of the security attributes of all services provided.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

9.4.2 Wireless Network Access

WIRELESS NETWORK ACCESS	
POLICY NUMBER: **9.4.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To protect the confidentiality, integrity, and availability of the State's network infrastructure and data from being compromised through the unauthorized exploitation of wireless network access technology; and to prohibit the deployment of open, unsecured wireless network access environments within the Maine IT Enterprise.

SCOPE

All Agencies of the State of Maine.

POLICY

The Office of Information Technology is responsible for specifying all policies and standards for implementing and operating any Wireless Local Area Network (WLAN) for any agency

within the scope of this document

GUIDELINES

The following guidelines should be considered when implementing and operating WLAN access:
- ➢ Take appropriate steps, including the implementation of strongest-available encryption, user authentication, and virus protection measures, to mitigate risks to the security of State of Maine data and information systems associated with the use of wireless network access technologies.
- ➢ Before implementing any new wireless technology, an assessment of the risks posed by the proposed use of wireless network access technology should be conducted.
- ➢ After assessment of the risks, appropriate steps should be taken to mitigate risks associated with the proposed wireless network access deployment.
- ➢ Periodic reviews should be conducted to ensure that the wireless network access technology is utilized in a secure manner and in compliance with all applicable established Standards.
- ➢ The deployment and operation of open, unsecured wireless network access technology is not recommended.

Operating System Hardening

Operating System hardening should include removal of default shares, strong administrator password, no unnecessary services/applications running on machine, etc.

Deployment of Most Secure Spread Spectrum Technology

Frequency Hopping Spread Spectrum should be employed rather than Direct Sequence Spread Spectrum as a means of more secure transmissions and less interference of transmissions.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

9.4.3 Networked Session Time-Out

NETWORK SESSION TIME-OUT	
POLICY NUMBER: **9.4.3**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To establish guidelines for activity timeout procedures for any networked session.

SCOPE

Sessions established by a logon via a directly attached or networked device. This policy does not

cover non-session activity such as browser based public access applications.

POLICY

Agencies must establish a standard length of time for inactivity that will cause a session to be terminated. Any session that exceeds the established length of time will automatically log the user off.

GUIDELINES

The level of risk associated with a logged in session should establish the length of time. In systems where the data is of a very critical nature the session timeouts should be short. Since short session timeouts can be very intrusive on staff productivity they should only be used when justified.

Longer logon session timeouts should be based on ensuring that logons are not kept overnight or through lunch hours. Longer timeouts are also allowable in areas where physical access to the logged in networked sessions is restricted to valid users.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

9.5 Operating System Access Control

9.5.1 Use of System Utilities

USE OF SYSTEM UTILITIES	
POLICY NUMBER: **9.5.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance for which types of users may use local system utilities. This policy also provides for the methods by which system utilities are made available on a system.

SCOPE

Types of system utilities and applications that are considered atypical for use by average users but typical for administration use by privileged users.

POLICY

System utilities will be available only to those users who have a business case for accessing the specific utility.

GUIDELINES

Systems that have been configured for best practices will typically follow these procedures:
 ➢ Using any system level utility will involve some form of user authentication.
 ➢ The system utilities will be segregated from other general user executables.
 ➢ The use of system utilities will be limited to a subset of authorized users with specific training and privileged user access.
 ➢ System Utility Use Logging.
 ➢ A document describing what system utilities are available for what purpose and what users may access them.
 ➢ Hardening of the operating system to remove any utilities not deemed necessary for the continued use of the system.
 ➢ Time constraints on when certain utilities may be used.

Operating System Differences

Various operating systems will have significantly different types of utilities and control methods. Controls applied to system level utilities will vary with the type of operating system involved. In any operating system care should be taken to limit user access to only those things that are really part of that users need for system access. In systems where diagnostic, network, change control and administrative utilities exist the average user account should not have access to execute or display the locations of these utilities. Trusted user access to system utilities should be done through individual user accounts with privileged user access and granted only based on the best practices security principle of least privilege. Where possible the use of these utilities should be logged.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

9.6 Application Access Control

9.6.1 Information Access Restriction

INFORMATION ACCESS RESTRICTION	
POLICY NUMBER: **9.6.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To prevent unauthorized access to information held in State of Maine computing resources. Any information held in a State of Maine computing resource should be protected from unauthorized access unless specifically designated for public dissemination.

SCOPE

All Agencies of the State of Maine. Any information held in non-public access areas of any

State of Maine computing system.

POLICY

> *All applications must have access controls unless specifically designated as a public access resource.*

GUIDELINES

User Access

State of Maine computing resources that provide applications to users should have controls that limit application access to only those users properly designated. The designation of which users should have access to specific applications should be based on business access control policy as formed by the Agency and its security administrator. Access to any application should be denied by default unless a need for access can be demonstrated. Any individual user should have specific controls limiting the rights to 'read,' 'write,' 'execute,' and 'delete' based on ownership of the information. Where resource ownership is shared the rights to modify the data should be based on a business decision of the Agency management.

System Configuration

Any State of Maine computing resource should provide protection from unauthorized access to any application or utility that can override application or system access controls.

Any system should be sufficiently secured to prevent compromising the applications or data of other systems it shares resources with.

Any system configuration should be able to limit access to information to only the owner of that information; other properly designated users, or defined groups of users.

Access to "system help' that would provide information on how to override existing security measures should be secured.

Controls should exist to limit the ability of the user to display, transmit, or use the output of any application only in ways approved by the Agency business management.

Public Access

Where systems are providing access to State of Maine resources to the general public, the information designated as public should be segregated from all non-public resources in specially designated public domain resource configurations.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

9.6.2 Limitation of Connection Time

LIMITATION OF CONNECTION TIME	
POLICY NUMBER: **9.6.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To further enhance the security of critical applications and data by implementing a 'period of valid connection' from specific connection types. By specifying times when a logon will be accepted from specific users and specific locations the overall security of a system is further enhanced.

SCOPE

Critical applications where the systems involved are configurable to allow for 'time of day' limitations on user logins. Data communications from other computer systems may also be controlled by 'time of day' restrictions.

POLICY

When deemed necessary, user logins and data communications must be restricted by time and date configurations that limit when connections will be accepted.

GUIDELINES

User Logins

When critical data and applications warrant above average security the use of a timed login is appropriate. Timed logins defines a period of time during the day and days of the week when logins will be accepted from specific users. Very often these timed restrictions are used in conjunction with a Location restriction as well. By restricting the logins of specific users to specific time of the day a more controlled environment may be achieved. Timed restrictions are not appropriate where users are going to be very dynamic in when they attempt to login. Where a policy of timed logins has been implemented a request to override the timed login should be a matter of approval by the security administrator as well as business management.

Data Communications

In systems where data communications from other computing resources will be sending or receiving information into a secured system the receiving system should have a 'time window' opened to begin the transactions required to move the data. The time window should be opened to begin the process and close after the process completes. The time window should be sufficiently large enough to accommodate slight variations in system times. Data communications timed connection should be used in conjunction with known system identifications. Where timed connections are considered applicable the use of some form of

system identification procedure is also appropriate.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

9.7 Monitoring System Access and Use

9.7.1 Event Monitoring

EVENT MONITORING	
POLICY NUMBER: **9.7.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide for the tracking of computing resource activity that will benefit the disclosure of unauthorized activity. Logs should be kept and reviewed in sufficient detail to detect activity atypical to the local environment.

SCOPE

The tracking of security related events and the data logs produced by the tracking mechanisms.

POLICY

State of Maine computing resources must be monitored by appropriate personnel to detect deviations from authorized use.

GUIDELINES

Logon Monitoring

A user event logging system should contain at a minimum the following information:
- ➢ User ID.
- ➢ Dates and times of logon and logoff.
- ➢ Logon method, location, terminal identity (if possible), Network address.
- ➢ Records of successful and unsuccessful system access attempts.
- ➢ Records of successful and rejected data access and other resource access attempts.

Log Archiving

The office of Information Technology will set minimum policy for the retention of logs. Individual agencies may specify greater retention based on agency need, or legal requirements. In all cases, the length of retention should reflect the availability of resources and the need to track historical information. The retention of logs should also reflect the possibility of providing evidence in future investigations. The storage and access to the logs should be sufficient to meet

the requirements of evidence collection.

Data Access Events

Where specific applications produce access event logs in addition to the system access logs the two logs should be archived in such a way as to make cross correlation possible.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

9.7.2 Monitoring System Use

MONITORING SYSTEM USE	
POLICY NUMBER: **9.7.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To ensure that there are adequate procedures in place to monitor the use of State of Maine computing resources. These procedures exist to ensure that the resources are being used in accordance with State of Maine, Federal, and Agency policy.

SCOPE

All Agencies of the State of Maine.

POLICY

Where appropriate and necessary, Agencies must establish procedures to monitor the events and activities of users accessing resources.

GUIDELINES

The areas of concern for monitoring on any specific system should be established as the result of a risk assessment. The procedures for monitoring should be established to facilitate the discovery of attempts at unauthorized access.

When performing the risk assessment to determine the types of monitoring to be done the following criteria should be assessed:
- Authorized access including:
    - User ID.
    - Date and time of key events.
    - Types of events.
    - Files or resources accessed.
    - Programs, utilities, and applications.
- Privileged Operations:

- o Use of supervisor account.
- o System Start-up and Stop.
- o I/O device attachment/detachment.
- ➢ Un-authorized access attempts
  - o Failed attempts.
  - o Access policy violations and notifications network gateways and firewalls.
  - o Alerts from proprietary intrusion detection systems.
- ➢ System alerts or failures, such as
  - o Console alerts or messages.
  - o System Log exceptions.
  - o Network management alarms.

Review of Monitoring Log Results

The log files produced by the monitoring systems should be reviewed on a periodic basis to determine if illicit activity has been taking place. The log files themselves should be secured in such a way as to prevent un-authorized alterations of the log files.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

9.7.3 Password Management Systems

PASSWORD MANAGEMENT SYSTEMS	
POLICY NUMBER: **9.7.3**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To describe the capabilities for password management to provide sufficient password security for computing resources in the State of Maine.

SCOPE

Any computing and networking resources connected to the State of Maine Wide Area Network. This policy covers the method of ensuring that passwords are of a sufficient quality to be considered safe to use.

POLICY

Password management systems must be deployed, where feasible, to provide a reliable, effective method of ensuring the use of high quality passwords.

GUIDELINES

Password Testing

The information technology security officer should ensure that all password files in use within a given environment undergo a periodic review to determine the vulnerability of passwords in use on a system.

Physical Password Security

Within any specific computing environment the ability of general users to access the files containing passwords should be limited. Password file access should be monitored for unauthorized activity.

Best Practice Features of Password Management

- ➢ Individual passwords should be unique per user and be accessible for accountability.
- ➢ Provide for creating high quality passwords.
- ➢ Allow users to create their own passwords and include a confirmation method for possible input errors.
- ➢ Where users maintain their own password, enforce password change schedules and password policies.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

9.8 Mobile Computing and Teleworking

9.8.1 Mobile Computing

MOBILE COMPUTING	
POLICY NUMBER: **9.8.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To ensure that mobile computing does not compromise the security of the systems being used.

SCOPE

Situations where connecting to State of Maine computing resources is done via some remote connection method. Typically this is via a telephone dial-up or Internet connection.

POLICY

Agencies shall adhere to the Remote Access implementation standards provided by the Office of Information Technology when requiring remote access to State of Maine Wide Area Network (WAN), and its connected resources.

GUIDELINES

When allowing remote access to internal systems a risk analysis should be performed that determines what methods of access are compatible with the required security levels of the systems being connected too. Requirements for specific connection methods or the use of cryptographic techniques should be clearly stated and enforced. The remote access risk analysis should result in a documented policy regarding the approved methods of remote connection.

User Education

Users of mobile computing access should be educated in the risks associated with using remote access. Emphasis should be placed on the physical security of a logged in laptop or the security of the information held on a laptop left in an un-secured location. Users should be educated in the use of cryptographic data storage and appropriate uses of cryptographic techniques. Users should also be made aware of issues such as 'overlooking' where strangers may be able to watch a logon sequence or view proprietary information over the shoulder of a valid user. Prior to allowing a user remote access some training should be provided that raises the security awareness level of the remote user.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

REFERENCES
1. **Policy to Safeguard Information on Portable Computing and Storage Devices** - http://www.maine.gov/oit/oitpolicies/SafeguardingPolicy_Final.htm

9.8.2 Teleworking

TELEWORKING	
POLICY NUMBER: **9.8.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance on security issues involved in teleworking.

SCOPE

Situations where agencies of the State of Maine allow users to work from locations that are not within an Agency managed or controlled facility

POLICY

Where Agencies have approved teleworking, that environment must include security features and services to ensure that State of Maine information resources are not compromised.

GUIDELINES

Where any Agency has made a determination that it would benefit from the use of teleworking facilities, the use of those facilities must meet the same security standards as normal internal facilities. The following criteria are typical to that evaluation:
  ➢ Can the teleworking site meet or exceed current physical security policy for internal systems?
  ➢ Is the proposed teleworking site environment conducive to a working environment that will promote staff productivity?
  ➢ Are the networking and communications systems reliable, robust and secure enough to meet current security policy for data communications?
  ➢ Is physical access to the teleworking environment secure enough to ensure no compromise of other State of Maine computing resources connected to it?
  ➢ Does the teleworking environment provide sufficient secure storage space for staff materials and equipment?
  ➢ Does the local environment have provisions for securing any unused network connections into the State of Maine networked infrastructure?
  ➢ Does the teleworking environment have timely procedures for revoking access to its facilities as needed?

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

10. Systems Development and Maintenance

10.1 Security Requirements of Systems

10.1.1 Security Requirements Analysis and Specification

SECURITY REQUIREMENTS ANALYSIS AND SPECIFICATION	
POLICY NUMBER: **10.1.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance for defining security related business requirements for new systems or enhancements to existing systems. These business requirements should specify and define the type and method of controls (automated and manual) to be incorporated into the systems, along with the scenarios of their expected use.

SCOPE

New information systems or revisions to existing State of Maine information systems

POLICY

> *The business requirements definition phase of system development must include a review to ensure that the system adheres to applicable security policies and standards.*

GUIDELINES

Business requirements for system development should include specifications for security controls. These specifications should address both automated controls and manual controls to be implemented. When implementing 'off the shelf' solutions, similar considerations should be part of the evaluation.

The security-related requirements of a system should:
- ➢ Reflect the sensitivity of the types of information to be handled by the system.
- ➢ Include a risk analysis that documents the types of risk associated with the system.
- ➢ Consider all pertinent data security standards that may affect security requirements (e.g., HIPPA and Federal Law Enforcement).

A minimum list of issues to be addressed by security requirements follows:
- ➢ Access controls (mandatory or discretionary).
- ➢ Administrator controls.
- ➢ Data classifications.
- ➢ Data encryption.
- ➢ Data output access.
- ➢ Data storage recovery.
- ➢ Data storage reliability.
- ➢ Network security.
- ➢ Operating system configuration.
- ➢ Physical security of system devices.
- ➢ System level access.
- ➢ System- to- System identification.
- ➢ User access methods.
- ➢ User account configuration.
- ➢ User identification.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

10.2 Security In Application Systems

10.2.1 Data Validation

DATA VALIDATION	
POLICY NUMBER: **10.2.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance in meeting the information security requirements of application design. Designing controls into applications will ensure that each level or type of information access is secured to a consistent level. Controls on how data is input, output, accessed and processed are essential to a secure computing environment.

SCOPE

New information systems or revisions to existing State of Maine systems

POLICY

> *Data input to application systems must be validated to ensure that it is correct and appropriate.*

GUIDELINES

Application design efforts range from an extremely complex multi-developer application or a small script used to parse data prior to populating a database. In either case, security-related issues for handling the data should be considered. To manage access, ownership of the data should be clearly established. However, applications should not subvert existing security controls in an attempt to make data access more convenient. Security policies should be reviewed during the design phase of an application; if there are questions, the information technology security officer should be contacted for assistance.

Checks should be applied to the input of business transactions, standing data (names and addresses, customer reference numbers) and parameter tables (prices, currency conversion rates, tax rates). The following controls should be considered:
  ➢ Dual input or other input checks to detect the following errors:
    o Out-of-range values.
    o Invalid characters in data fields.
    o Missing or incomplete data.
    o Exceeding upper and lower data volume limits.
    o Unauthorized or inconsistent control data.
  ➢ Periodic review of the content of key fields or data files to confirm their validity and integrity.
  ➢ Inspecting hard-copy input documents for any unauthorized changes to input data (all changes to input documents should be authorized).
  ➢ Procedures for responding to validation errors.
  ➢ Procedures for testing the plausibility of the input data .
  ➢ Defining the responsibilities of all personnel involved in the data input process.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

10.3 Cryptographic Controls

10.3.1 Cryptographic Controls

CRYPTOGRAPHIC CONTROLS	
POLICY NUMBER: **10.3.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance on application security design requirements that may involve the use of cryptographic security controls. Cryptography protects information from unauthorized access and disclosure. Where the confidentiality, authenticity, or integrity of information is critical, the use of cryptographic controls may be warranted.

SCOPE

New State of Maine information systems or modifications to existing systems

POLICY

The decision to use cryptographic controls will be based on the level of risk of unauthorized access and the sensitivity of the data that is to be protected.

GUIDELINES

Cryptographic controls are used to protect sensitive information. They typically use software keys that must be managed to ensure the integrity of the information.

The choice of the type and quality of the encryption should be based on risks and the level of data classification, with consideration given to compatibility of existing data storage systems. Choice of encryption should also consider issues regarding the use of encryption in foreign countries, trans-border communication of encrypted material, and import and export law regarding encryption technology. The requirement for cryptographic controls for the data should be explicit, and the corruption additional processing due to the use of encryption must be considered in the overall system design. Wireless communications, for example, should have encryption services enabled to prevent interception and unauthorized access to State information resources.

When prescribing the use of cryptographic services, the following issues should be considered:
- ➢ Approach for determination of level of cryptographic services to be used.
- ➢ The approach to 'key' management, including methods to deal with the recovery of encrypted information in the case of a lost, compromised or damaged key.
- ➢ Roles and responsibilities, e.g. who is responsible for:
  - o The implementation of policy.
  - o 'Key' management.
- ➢ How to determine the appropriate level of cryptographic protection.
- ➢ The standards to be adopted for the effective implementation of the technology for the

transmission and classification of data; (which solution is used for which business process).

Data Encryption

When deciding to use encryption, the issues regarding the technical parameters of encryption affect the technology selected. Requirements to encrypt entire file structures, single data files, data communications, entire hard drives, email content, databases, signatures and application code will all dramatically affect the type of encryption and product used.

Digital Signatures

Digital signatures provide a method for adding assurance that a specific email or electronic document is intact and maintains its original integrity. Digital signatures can be applied to many forms of documents and messages being processed electronically.

The public and private keys (special encrypted files that require a password to use) require special protection to ensure that they are not used to "sign" things without authorization. Private keys should be issued to individuals and not shared with anyone. The location of private keys should remain physically and logically secure.

When designing an application to use digital signatures, consideration should be given to the type and quality of the signature algorithm used and the length keys to be used. The processing of encryption/decryption and digital keys will put a load on a system and should be considered in the system sizing. Cryptographic keys used for digital signatures should be different from those used for encryption.

The use of digital signatures should be reviewed with consideration given to relevant legislation that describes the conditions under which a digital signature is legally binding. Legal advice should be sought regarding the laws and regulations that might apply to the organizations intended use of digital signatures.

Non-Repudiation Services

Non-repudiation services exist to provide a method of resolving a dispute regarding an event. The use of non-repudiation services can help establish evidence to substantiate whether a particular event or action has taken place, e.g. denial of sending a digitally signed instruction using electronic mail. These services are based on the use of encryption and digital signature techniques.

Note that the technical term 'non-repudiation' in this context is not synonymous with the legal definition. If electronic non-repudiation is to be used in a context that may involve legal action, the use of electronic non-repudiation techniques may not meet a local legal standard. Legal counsel should be sought to determine the limits of using electronic non-repudiation services.

Key Management

Digital signatures and other forms of encryption use electronic cryptographic keys. The effective management of keys is essential to creating the 'trust model' that forms the basis of digital signatures and ensuring that the encrypted information is secure from disclosure. Any compromise of the keys may lead to compromise of the confidentiality, authenticity, and/or integrity of information.

A key management system should support two basic types of cryptographic techniques:
➢ Symmetric key encryption involves two or more parties that share the same key. These keys are used to encrypt and decrypt information. Compromise of a symmetric key could lead to the introduction of information into a system from an unauthorized source.
➢ Public key techniques involve the use of a key pair: a public key and a private key.

All keys should be protected against modification or destruction. Private keys need protection from unauthorized disclosure.

A key management system should be based on information technology security standards, procedures and methods for:
➢ Generating keys for different cryptographic systems and different applications.
➢ Generating and obtaining public key certificates.
➢ Distributing keys to intended users, including how keys should be activated when received.
➢ Storing keys, including how authorized users obtain access to keys.
➢ Changing or updating keys including rules on when keys should be changed and how this will be done .
➢ Procedures for dealing with compromised keys.
➢ Revoking keys including how keys should be withdrawn or deactivated, for example when keys have been compromised or when a user leaves an organization (in which case keys should be archived).
➢ Recovering keys that are lost or corrupted as part of business continuity management, for example recovery of encrypted information.
➢ Archiving keys, e.g. for information archived or backed up .
➢ Key destruction.
➢ Logging and auditing of key management related activities.

To further reduce the likelihood of key compromise, keys should have defined activation and deactivation dates to limit the time for which they can be used.

The issuing of public and private keys should include a process of physical identification of the user requesting the keys. Issues related to liability, reliability of services and response times should be addressed with providers of public key technology.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

REFERENCES
1. **Policy to Govern PKI Security Requirements and Certification Policies** -
   http://www.maine.gov/oit/oitpolicies/PKIpolicy.htm
2. **State of Maine PKI Security Policy Requirements** -
   http://www.maine.gov/oit/oitpolicies/PKIrequirements.htm
3. **State of Maine X.509 Certification Policies and Practices Statement** -
   http://www.maine.gov/oit/oitpolicies/certstatement.htm

10.4 Security of System Files

10.4.1 Control of Operational Software

CONTROL OF OPERATIONAL SOFTWARE	
POLICY NUMBER: **10.4.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance regarding securing operating system files and application software. The securing of these files further ensures that only authorized activity may take place on a system.

SCOPE

New State of Maine information systems or modifications to existing systems.

POLICY

The operating system files and application software must be secured from unauthorized use or access.

GUIDELINES

Desktop systems should be prohibited from using software that has not been approved and licensed for use. Periodic auditing of software on desktop systems should be performed to ensure that only authorized and licensed software is in use.

Systems that have been classed as 'production' should have a rigorous change management process in place. Approvals for change at the operating system level should include security administration. The operating system files should be minimized to only those files required for the purpose the systems is designed to perform. Prior to placing a system into change management the operating system files should be audited for authenticity and directory structures. The production system should be monitored for changes during operation and audited on a regular schedule. File systems of a production system that are application specific will contain some level of dynamic data. Auditing dynamic data areas should be done for plausibility, e.g. the directory structures contain only expected files with typical permissions.

Static application data areas (e.g. the static information used to populate a website outside of any dynamic data available there) of the file system should be under change management with an

approval process that involves the application owners. All change control operations should include roll back plans and event logging.

When establishing controls on production or operational systems the following should be considered:

> The designated administrator upon appropriate change management approval should only perform the updating of operational program libraries.
> If possible, production systems should only hold operationally relevant code and data.
> Executable code should not be installed on a production system until evidence of successful testing and user acceptance has been obtained.
> An audit log should be maintained of all updates to operational systems files.
> Previous versions of software should be retained as a contingency measure.

The differences in control procedures available between enterprise class (mainframe, large Unix), medium class (Unix, AS400) and small (NT, 2000) are profound. Establishing change control and good production management on small systems is the most difficult to manage. An established method of change control is appropriate to any class of system. The level of control is where the differences between systems will occur. Desktops should only be under rigorous change control when the business and security needs justify the expense and lack of convenience to users.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

10.4.2 Protection of System Test Data

PROTECTION OF SYSTEM TEST DATA	
POLICY NUMBER: **10.4.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance for the securing data generated as a result of system testing. The data that occurs as a result of testing, auditing and diagnosing problems on a production system pose a significant source of proprietary information about a system. Systems containing sensitive information should require very careful management of test data to prevent unauthorized disclosure.

SCOPE

New State of Maine information systems and/or making modifications to existing systems.

POLICY

> *Data that results from testing must be handled, stored, and disposed of in the same manner and using the same procedures as used for production data.*

GUIDELINES

When systems are tested, the resulting data and test results should be handled as sensitive information until the information can be disposed of properly. Programs specifically used for testing should be protected from casual access. Diagnostic routines and administrative scripts should be secured under the same conditions as other system utilities. System tests should be performed on data that is constructed specifically for that purpose. System testing should not be performed on operational data unless the required safeguards are in place. The following controls should be applied to protect operational data when tests are conducted.

➢ The access control procedures, which apply to operational application systems, should also apply to test applications systems.
➢ There should be separate authorization, each time operational information is copied to a test application system.
➢ Operational information should be erased from a test application system immediately after the testing is complete.
➢ The copying and use of operational information should be logged to provide an audit trail.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

10.4.3 Access Control to Program Source Libraries

ACCESS CONTROL TO PROGRAM SOURCE LIBRARIES	
POLICY NUMBER: **10.4.3**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance on the controls for access to program source libraries on systems using them

SCOPE

Systems that use program source libraries as an operational component of the operating system on State of Maine computing resources.

POLICY

> *Access to program source libraries must be protected to ensure access by only authorized users.*

GUIDELINES

Certain types of computing systems (typically mainframes) have program source libraries loaded

onto the system when the operating system is loaded. In situations where the system is to be considered a production system and under change control management, the program source libraries should be removed unless specifically required for some purpose. Great care should be taken to make sure that the libraries are archived based on the exact versions of software actually running. These guidelines are not intended to apply to medium class and small systems. In midrange systems, this process is handled by securing the kernel and binary files. In small systems the software vendor, for example Microsoft, generally holds the program source code.

Strict control should be maintained over access to program source libraries with the following considerations:

➢ Where possible, program source libraries should not be held in the production systems.
➢ A program source librarian (administrator) should be appointed for each application.
➢ IT support staff should not have unrestricted access to program source libraries.
➢ Programs under development or maintenance should not be held in production program source libraries.
➢ The updating of program source libraries and the issuing of program sources to programmers should only be performed by the appointed librarian upon authorization from the IT support manager for the application.
➢ Program listings should be held in a secure environment.
➢ An audit log should be maintained of all accesses to program source libraries.
➢ Multiple updates to any production module between backup executions should be prohibited.
➢ Old versions of source programs should be archived, with a clear indication of the precise dates and times when they were operational, together with all supporting software, job control, data definitions and procedures.
➢ Maintenance and copying of program source libraries should be subject to strict change control procedures.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

10.5 Security in Development and Support Process

10.5.1 Change Control Procedures

CHANGE CONTROL PROCEDURES	
POLICY NUMBER: **10.5.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance on change controls for the development, implementation, and support of software and hardware.

SCOPE

New State of Maine information systems or modifications to existing systems.

POLICY

Hardware and software proposed for use in State of Maine computing resources must have documented change control procedures to ensure proper versioning and implementation.

GUIDELINES

The development of software for State of Maine represents a security risk in that unauthorized access to the design, code, libraries and databases may allow either compromise of the new code or provide information for later incursions.

The control and maintenance of data communications infrastructure also requires a change control process to ensure continued availability of communications resources. Support staff involved in the ongoing support of data communications should have a change control and approval process documented.

Change Control Procedures

The project and support environment for software development should be controlled to prevent unauthorized access. Review of the development infrastructure should be performed by information technology security officer to determine the quality of the security controls in place. The development file servers, compile engines, library storage and test systems should be physically secure.

In order to minimize the possible corruption of information systems there should be strict control over the implementation of changes. Formal change control procedures should be enforced.

Mainframe Systems

In mainframe systems software analysts should be given access to only those parts of the systems they actually need for their work. The process of writing system application code on mainframe systems should follow the change control procedures. New system code should not be introduced into the system without having been rigorously tested and approved. Wherever possible, application and system support change control should be integrated.

This process should include:
➢ Maintaining a record of agreed authorization levels.
➢ Ensuring changes are submitted by authorized users.
➢ Reviewing controls and the integrity procedures to ensure that they will not be compromised by the changes.
➢ Identifying all computer software, information, database entities and hardware that require amendment.
➢ Obtaining formal approval for detailed proposals before work commences.
➢ Ensuring that the authorized user accepts changes prior to implementation.

➢ Ensuring that the implementation is carried out to minimize disruptions.
➢ Ensuring that the system documentation set is updated on the completion of each change and that old documentation is archived or disposed of.
➢ Maintaining a version control for all software updates.
➢ Maintaining an audit trial of all change requests.
➢ Ensuring that operating documentation and the user procedures are changed as necessary to be appropriate.

Midrange Systems and Small Servers

Midrange software development differs from Mainframe in that the typical separation of applications and operating system software is very distinct, such that there is no operating system development involvement in medium class range application development.

Change control procedures for loading new or updated application software on medium class systems should follow rigorous control. Application and full systems testing should still take place prior to implementing on production systems. The executable code should be minimized to only that code which is required to meet the production goals.

The administrator of that system should carry out loading of application software onto a production system. Application developers should not have administrator access to the production systems.

The new application should be fully documented as to:
➢ Application function or purpose.
➢ Special system tuning required.
➢ Special application user accounts required.
➢ File and directory structures.
➢ Super user accounts.
➢ Account and file permissions.
➢ Network ports to be used.
➢ System libraries required and versions.
➢ Device files to be created.
➢ Data storage requirements.
➢ Kernel changes, if any.
➢ Scheduled tasks.

Desktop Systems

Desktop software development typically has a distinct separation of applications and operating system software. Because the new or modified software may need to be installed on a number of individual desktop systems, change control should focus on:
➢ Thoroughly testing the install or upgrade procedure on all types of user desktops that will be affected.
➢ Notifying users and help-desk staff ahead of time of the upcoming change so that the work can be scheduled to minimize user disruption.

➢ If support personnel are going to visit each user desktop, users should be notified well in advance so they are prepared.
➢ If the users are going to be involved in the change, their effort should be minimized through such things as automated install procedures, server-based installs, etc.
➢ Possible extra on-call support during the rollout to answer questions.
➢ Follow-up with users to be sure the new or upgraded software has been successfully installed.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

10.5.2 Review of Operating System Changes

REVIEW OF OPERATING SYSTEM CHANGES	
POLICY NUMBER: **10.5.2**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance on the process of changing or upgrading production operating systems. Throughout the life cycle of a production system there will be legitimate reasons to upgrade the operating system. When these upgrades are proposed, a review of the impact to existing business functionality and security should be performed.

SCOPE

New systems for the State of Maine, and modifications to existing systems.

POLICY

When preparing to upgrade an operating system on a production computing resource, the process of testing and approving the upgrade must be developed to minimize security risks and disruption to the production environment.

GUIDELINES

There are many legitimate cases for upgrading or patching the operating system of a computing resource, e.g. security patches, performance patches, maintenance upgrades, etc. When these conditions occur the process of reviewing the effects of the patch or upgrade should be thoroughly tested and reviewed prior to making the change.

In the best of circumstances, a completely redundant test system with identical system load and hardware compatibility will be available to test the new code. When a completely redundant system is not available, then unit testing should be done in a way that as closely as possible approximates conditions of the production system. Immediately prior to loading the new code a system backup and database backup should be performed. In cases where the business

availability of the applications will be affected, the upgrade should be scheduled to take place at a time when the impact will be the least.

In systems where an operating system upgrade will involve a re-boot of the system, special considerations should be taken to identify and properly close out any running tasks. In particular, if the system is running a sophisticated database with transactional capabilities that require multiphase commit of data, the data base administrator should be part of the upgrade team. Any applications that require special handling in how they are brought back into production mode should have an application administrator on hand to help guide the process.

When trying to do multiple changes to a system at one time, care should be taken to ensure the proper order of changes. Some upgrades and patches will require that others patch or upgrades be loaded first. In general it is not considered a good practice to change multiple aspects of a system without system testing to verify each change individually.

Prior to the upgrade, a series of test programs and procedures should be created to verify the capabilities of the system after the upgrade. The tests should be designed to verify that all operational characteristics of the system are nominal. A plan for backing the changes out and returning to the current state should be prepared in case of unexpected results.

Upgrades should be scheduled in consultation with business management to minimize the impact to the business. The administrators of other systems that communicate regularly with the system to be upgraded should be notified of the impending downtime. If an alerting system or network operations center monitors the availability of resources, they should be notified as well.

Typically a series of notifications regarding scheduled downtime should be sent out as early as possible before the actual upgrade. Within the last 24 hours before the upgrade at least three reminders should go out during the period. If the system supports a session-less server (e.g. Web server) a reminder should be posted on the primary page of the website.

The review process that provides a technical approval of an upgrade should include the following:
  ➢ Review of applications control and the integrity procedures to ensure that they have not been compromised by the operating system changes.
  ➢ Ensuring that the annual support plan and budget will cover reviews and system testing resulting from operating system changes.
  ➢ Ensuring that notification of operating system changes is provided in time to allow appropriate reviews to take place before implementation.
  ➢ Ensuring that appropriate changes are made to the business continuity plans.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

10.5.3 Restrictions on Changes to Software Packages

RESTRICTIONS ON CHANGES TO SOFTWARE PACKAGES	
POLICY NUMBER: **10.5.3**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To cover the use of purchased software and changes to executable code provided by a vendor.

SCOPE

Purchased software used for or by State of Maine computing resources.

POLICY

Software provided by third party vendors, and related customization, must include sufficient documentation to satisfy applicable audit requirements and security policies and procedures.

GUIDELINES

Third party software should normally be used as the vendor supplied it. Modifications to the executable code should be prevented unless provided by the vendor in the form of a patch or upgrade. Modifications to vendor supplied software packages that are provided via 'open-source' resources should not be allowed on state systems unless specifically supported and supplied by the original vendor. Where circumstances occur that make it essential to change a software package, the following points should be considered:
 ➢ The risk of built-in controls and integrity processes being compromised.
 ➢ Whether the consent of the vendor should be obtained.
 ➢ The possibility of obtaining the required changes from the vendor as standard program updates.
 ➢ The impact if the organization becomes responsible for the future maintenance of the software as a result of changes.
 ➢ The possibility of undetected security compromises existing in the new code.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

10.5.4 Malicious Code

MALICIOUS CODE	
POLICY NUMBER: **10.5.4**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To avoid compromise of software introduced in an unauthorized manner.   This compromise may take the form of Trojan Horse code, "time or logic bombs", or viruses.

SCOPE

All systems operated by Agencies of the State of Maine.

POLICY

> *Systems must be hardened and logs monitored to ensure the avoidance of the introduction and exploitation of malicious code.*

GUIDELINES

The avoidance of malicious code is dependant on multiple factors, a major one being an educated user population as the first line of defense. When users are connected to the Internet via a local area network they should be educated on safe practice when using resources from the internet. Email systems are also a method of incursion for malicious code. Email containing binary attachments that are executable should not be opened unless the sender is known, the file is expected, or the file screened through approved anti-virus software.

In providing protection form malicious software activity the logical perimeter of a networked environment is the best practice for emplacement of detection and protective devices. Eliminating the threat as it arrives at the first level of communication into an environment is the most effective method for detection and prevention.

Free "open-source" software available on the internet may result in the inadvertent introduction of malicious code and should not be used unless approved by appropriate management.

The following guidelines should be considered to avoid compromise through malicious code:
- Buy programs from only reputable sources.
- Use evaluated third party products.
- Inspect all source code before operational use.
- Control access to, and modification of, code once installed.
- Use staff screened for appropriate background to work on key systems.
- Adhere to sound email policy regarding attachments and unknown email source.
- Limit how software may be executed on server class systems.
- Monitor network communications going to the Internet for atypical behavior.
- Use virus protection and intrusion detection software.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

11. Disaster Recovery and Business Continuity

11.1 Aspects of Disaster Recovery and Business Continuity

11.1.1 Disaster Recovery and Business Continuity Planning

DISASTER RECOVERY AND BUSINESS CONTINUITY PLANNING	
POLICY NUMBER: **11.1.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To ensure that state government agencies develop and maintain disaster recovery and business continuity plans and processes to allow them to continue to deliver their essential business functions despite damage, loss, or disruption of State of Maine information systems due to the unexpected occurrence of a natural or man-made emergency or disaster.

SCOPE

All State of Maine agencies. The principles associated with this policy apply to Agency operations as a whole. However, the scope of this policy is limited to plans and processes that address unavailability of information systems due to unforeseen events.

POLICY

Each Agency must develop, periodically update, and annually test disaster recovery and business continuity plans designed to ensure the availability and security of the Agency's essential services and communications in the event of an adverse impact to such Agency's information systems due to a natural or man-made emergency or disaster event.

GUIDELINES

Risk Assessment

Risk assessments should be conducted and formally documented to assess the risks and their potential impacts to the organization. With each risk, an analysis of the likelihood of an event should be determined and prioritized in such a manner so that methods of mitigation can be explored. Risk assessments should include both technical and environmental threats to software (data and applications), hardware (including operating systems) and procedures. Risk assessments should be reviewed annually and updated as required.

Impact Analysis

An impact analysis provides an understanding of the effect that an interruption will have on the organization. These should include both long and short-term interruptions of minor and major incidents.

Alignment to Business Strategy

Business continuity plans should be created to support the organizations business objectives and priorities. This should be reflected in procedures supporting application and data back-up

requirements and procedures required for system restoration. Specific considerations to include in data back-up and testing should include:

- ➢ Consistent implementation of data back-up for critical systems that include:
  - o Standard back-up schedules.
  - o Consistent data vaulting procedures.
  - o Regular, formal back-up testing and restores, including applications.
  - o Service Level Agreements (SLAs) that identify responsibility for data and application back-up, restoration and testing.
- ➢ Development of a redundant network architecture to eliminate a single point of failure for data communications.
- ➢ Determination and selection of an alternative processing facility, if required.

Alignment of Business Continuity Strategy

A strategy for business continuity should be agreed to by the organization. This will ensure that each part of the organization is supporting one plan and one strategy.

Testing and Updating the Plan

Business continuity plans should be tested annually to determine effectiveness. Schedules and times should be based upon changes to the environment and training needs for the staff involved. Updates to the plans are necessary to keep information and processes accurate. Consideration should be given to digitizing or duplicating irreplaceable Agency physical documentation for off-site archival.

Management of the Plan

Business continuity needs to be supported at the appropriate level in the organization. Responsibilities for the plan will be distributed across the organization and therefore require senior level support. Management should ensure that the organization's processes are incorporated into the structure of the plan.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

12. Compliance

12.1 Compliance with Legal Requirements

12.1.1 Compliance with Legal Requirements

COMPLIANCE WITH LEGAL REQUIREMENTS	
POLICY NUMBER: **12.1.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance in operating State of Maine information systems in compliance with applicable local, State and Federal laws and regulations.

SCOPE

State of Maine information, applications, and communications systems

POLICY

> *Information security policies must comply with State and Federal regulations. Agencies must include these regulations in employee security awareness and compliance training*.

GUIDELINES

State Information

The State has a responsibility to ensure that the public is allowed the right to examine specific information. Each entity within the State should provide appropriate access while, at the same time, ensuring protection from unauthorized disclosure and alteration. The Chief Information Officer has the responsibility for establishment of statewide policies, including information security. However, each Agency is responsible for developing its own specific procedures necessary to ensure operational compliance with State and Federal requirements, such as HIPAA, FERPA, COPPA, Gramm-Leach Bliley Act and CJIS).

Acceptable Usage

The information processing resources of the State of Maine are provided for the business purposes of the State. Use of State information resources must comply with specific regulations for their proper use. Requirements for compliance for information security responsibilities should be presented and signed by each employee.

Security Awareness

Awareness and training should be provided for State employees, commensurate with their information processing and handling responsibilities. Compliance and permanence are predicated upon an understanding of information security policies and procedures by State employees, which are a critical element for a secure information-processing environment.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

REFERENCES
 1. **E-Mail Usage and Management Policy** -
    http://www.maine.gov/oit/oitpolicies/emailusagemanage.htm

2. **POLICY CONCERNING THE USE OF STATE-OWNED INFORMATION AND TECHNOLOGY (I.T.) AND RELATED COMMUNICATIONS EQUIPMENT** - http://inet.state.me.us/dafs/policies/itpolicy.html
3. **(EISD-SD-2008.04) Network Warning Banner on Acceptable Use of State Resources** - http://inet.state.me.us/oit/services/CoreTechnology/security/Security%20Directives/EISD%20Security%20Directive%20-%20EISD-SD-2008%2004.doc

12.2 Reviews of Security Policy and Technical Compliance

12.2.1 Reviews of Security Policy and Technical Compliance

REVIEWS OF SECURITY POLICY AND TECHNICAL COMPLIANCE	
POLICY NUMBER: **12.2.1**	EFFECTIVE DATE: December 19, 2002

PURPOSE

To provide guidance for ensuring that compliance issues regarding information security will be properly addressed.

SCOPE

Information systems operated by agencies of the State of Maine.

POLICY

Agencies must conduct annual reviews of written procedures and operations to ensure compliance with security policies and applicable standards.

GUIDELINES

Security Policy Compliance

Each State entity should ensure that periodic compliance audits and reviews are conducted in cooperation with State auditing personnel. Frequency of reviews should be based on the risk and criticality of the processing environment, major changes, or new State or Federal regulations.

Security compliance audits should be conducted with the assistance of a third party. The Office of Information Technology, other Agencies, or contracted support should be used. An audit or review conducted by another authority, such as the Internal Revenue Service, may substitute for this review if similar in scope.

Technical Compliance Evaluations

State of Maine information systems should be submitted to regular reviews of technical security audits. These reviews should be performed to determine current compliance with existing security implementation standards. Technical compliance evaluations are based on performing

various types of tests and examining configurations.

Compliance testing should identify weaknesses subject to exploitation, and qualify results as to the nature of criticality. Technical evaluations should be done in cooperation with operations personnel to avoid impact on productions environments. The handling of results and data obtained in such evaluations should comply with data classification restrictions.

AUTHORITY, ENFORCEMENT, EXCEPTIONS (see Section 1)

TERMS AND DEFINITIONS (see Section 2)

Revision History			
Rev.	Date	Reason for revision	Revisor
1.0	Dec. 19, 2002	Original	D. Hildebrand
1.1	Dec. 12, 2008	Changes made to reflect organizational changes in IT structure. BIS changed to OIT, ISPB changed to CIO, law references updated.	R. Witham
1.2	Jan. 1, 2009	Changed one occurrence of Office of Information Services to Office of Information Technology	R. Witham

APPENDIX A

Information Security Related Documents/Resources

- ➢ Office of Information Technology Policies
  - o Wide Area Network (WAN) Policy
  - o E-Mail Virus Action Plan

- ➢ State of Maine Information Technology Policies and Standards.

- ➢ State of Maine Information Technology Strategic Plan and Architecture.

- ➢ State Statutes
  - o Maine Public Records and Proceedings (MRSA, Title 1, Chapter 13)
  - o Maine Uniform Electronic Transaction Act (MRSA, Title 10 Chapter 1051)
  - o Maine Digital Signature Act (MRSA, Title 10, Chapter 1053)

- ➢ Federal Statutes
  - o Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA Patriot) Act of 2001
  - o Family Educational Rights and Privacy Act (FERPA)
  - o Health Insurance Portability and Accountability Act of 1996
  - o The Gramm-Leach-Bliley--Financial Services Modernization Act
  - o The Computer Matching and Privacy Protection Act of 1998 & Amendments of 1990
  - o The Children's Online Privacy Protection Act of 1998
  - o The Driver's Privacy Protection Act
  - o The Privacy Act of 1974
  - o The Fair Credit Reporting Act
  - o The Electronic Communications Privacy Act of 1986
  - o The Computer Fraud and Abuse Act of 1986